SINTEF

SINTEF A23413- Unrestricted

Report

ValidKI: A Method for Designing Indicators to Monitor the Fulfillment of Business Objectives with Particular Focus on Quality and ICT-supported Monitoring of Indicators

Author(s)
Olav Skjelkvåle Ligaarden, Atle Refsdal, and Ketil Stølen

SINTEF ICT
Networked Systems and Services
2012-10-01

SINTEF

SINTEF IKT
SINTEF ICT

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY

Telephone:+47 73593000
Telefax:+47 22067350

postmottak.IKT@sintef.no
www.sintef.no
Enterprise /VAT No:
NO 948 007 029 MVA

Report

ValidKI: A Method for Designing Indicators to Monitor the Fulfillment of Business Objectives with Particular Focus on Quality and ICT-supported Monitoring of Indicators

KEYWORDS:
Indicator,
Key indicator,
Business objective,
Quality,
ICT-supported monitoring,
Electronic patient record

VERSION
Final version

DATE
2012-10-01

AUTHOR(S)
Olav Skjelkvåle Ligaarden, Atle Refsdal, and Ketil Stølen

CLIENT(S)
Research Council of Norway

CLIENT'S REF.
180052/S10

PROJECT NO.
90B245

NUMBER OF PAGES/APPENDICES:
48/0

ABSTRACT
In this report we present our method ValidKI for designing indicators to monitor the fulfillment of business objectives with particular focus on quality and ICT-supported monitoring of indicators. A set of indicators is valid with respect to a business objective if it measures the degree to which the business or relevant part thereof fulfills the business objective. ValidKI consists of six main steps. We demonstrate the method on an example case focusing on the use of electronic patient records in a hospital environment.

PREPARED BY
Olav Skjelkvåle Ligaarden

SIGNATURE
Olav S. Ligaarden

CHECKED BY
Fredrik Seehusen

SIGNATURE

APPROVED BY
Bjørn Skjellaug, Research Director

SIGNATURE

REPORT NO. SINTEF A23413

ISBN 978-82-14-05579-5

CLASSIFICATION Unrestricted

CLASSIFICATION THIS PAGE Unrestricted

CONTENTS

ValidKI: A Method for Designing Indicators to Monitor the Fulfillment of Business Objectives with Particular Focus on Quality and ICT-supported Monitoring of Indicators

Olav Skjelkvåle Ligaarden*†, Atle Refsdal*, and Ketil Stølen*†
* Department for Networked Systems and Services, SINTEF ICT
PO Box 124 Blindern, N-0314 Oslo, Norway
E-mail: {olav.ligaarden, atle.refsdal, ketil.stolen}@sintef.no
† Department of Informatics, University of Oslo
PO Box 1080 Blindern, N-0316 Oslo, Norway

Abstract

In this report we present our method ValidKI for designing indicators to monitor the fulfillment of business objectives with particular focus on quality and ICT-supported monitoring of indicators. A set of indicators is valid with respect to a business objective if it measures the degree to which the business or relevant part thereof fulfills the business objective. ValidKI consists of six main steps. We demonstrate the method on an example case focusing on the use of electronic patient records in a hospital environment.

Keywords

Indicator, key indicator, business objective, quality, ICT-supported monitoring, electronic patient record

I. Introduction

Today's companies benefit greatly from ICT-supported business processes, as well as business intelligence and business process intelligence applications monitoring and analyzing different aspects of a business and its processes. The output from these applications may be indicators which summarize large amounts of data into single numbers. Indicators can be used to evaluate how successful a company is with respect to specific business objectives. For this to be possible it is important that the indicators are valid. A set of indicators is valid with respect to a business objective if it measures the degree to which the business or relevant part thereof fulfills the business objective. Valid indicators facilitate decision making, while invalid indicators may lead to bad business decisions, which again may greatly harm the company.

In today's business environment, companies cooperate across company borders. Such co-operations often result in sharing or outsourcing of ICT-supported business processes. One example is the interconnected electronic patient record (EPR) infrastructure. The common goal for this infrastructure is the exchange of EPRs facilitating the treatment of the same patient at more than one hospital. In such an infrastructure, it is important to monitor the use of EPRs in order to detect and avoid misuse. This may be achieved through the use of indicators. It may be challenging to identify and compute good indicators that are valid with respect to business objectives that focus on quality in general and security in particular. Furthermore, in an infrastructure or system stretching across many companies we often have different degrees of visibility into how the cooperating parties perform their part of the business relationship, making the calculation of indicators particularly hard.

In [1] we presented the method *ValidKI* (Valid Key Indicators) for designing indicators to monitor the fulfillment of business objectives with particular focus on quality and ICT-supported monitoring of indicators. ValidKI facilitates the design of a set of indicators that is valid with respect to a business objective. In this report we present an improved version of the method.

We demonstrate ValidKI by applying it on an example case targeting the use of EPRs. We have developed ValidKI with the aim of fulfilling the following characteristics:

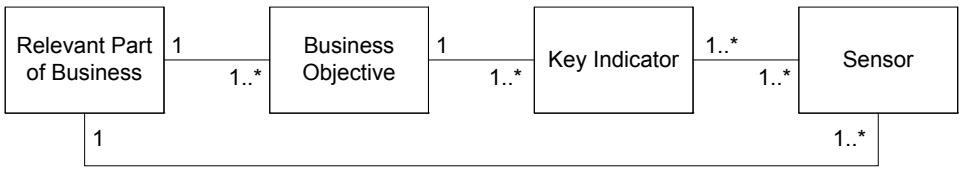

Fig. 1. The artifacts addressed by ValidKI

- **Business focus:** The method should facilitate the design and assessment of indicators for the purpose of measuring the fulfillment of business objectives with particular focus on quality and ICT-supported monitoring of indicators.
- **Efficiency:** The method should be time and resource efficient.
- **Generality:** The method should be able to support the design and assessment of indicators based on data from systems that are controlled and operated by different companies or organizations.
- **Heterogeneity:** The method should not place restrictions on how indicators are designed.

The rest of the report is structured as follows: in Section II we introduce our basic terminology and definitions. In Section III we give an overview of ValidKI and its six main steps. In Sections IV – IX we demonstrate our six-step method on an example case addressing the use of EPRs in a hospital environment. In Section X we present related work, while in Section XI we conclude by characterizing our contribution and discussing the suitability of our method.

II. Basic terminology and definitions

Hammond et al. defines indicator as *"something that provides a clue to a matter of larger significance or makes perceptible a trend or phenomenon that is not immediately detectable"* [2]. For example, a drop in barometric pressure may signal a coming storm, while an unexpected rise in the traffic load of a web server may signal a denial of service attack in progress. Thus, the significance of an indicator extends beyond what is actually measured to a larger phenomenon of interest.

Indicators are closely related to metrics. ISO/IEC/IEEE 24765 [3] defines metric as *"a quantitative measure of the degree to which a system, component, or process possesses a given attribute,"* while it defines attribute as *"the specific characteristic of the entity being measured."* For the web server mentioned above, an example of an attribute may be availability. An availability metric may again act as an indicator for denial of service attacks, if we compare the metric with a baseline or expected result [4]. As we can see, metrics are not that different from indicators. For that reason, indicators and metrics are often used interchangeably in the literature.

Many companies profit considerably from the use of indicators [5] resulting from business process intelligence applications that monitor and analyze different aspects of a business and its processes. Indicators can be used to measure to what degree a company fulfills its business objectives and we then speak of key indicators. Some business objectives may focus on business performance, while others may focus on risk or compliance with laws and regulations. We will in the remainder of the report refer to indicators as key indicators, since we focus on indicators in the context of business objectives.

A. The artifacts addressed by ValidKI

The UML [6] class diagram in Fig. 1 relates the main artifacts addressed by ValidKI. The associations between the different concepts have cardinalities that specify how many instances of one concept that may be associated to an instance of the other concept.

As characterized by the diagram, one or more key indicators are used to measure to what extent a business objective is fulfilled with respect to a relevant part of the business. Each key indicator is calculated based on data provided by one or more sensors. The sensors gather data from the relevant part of the business. A sensor may gather data for more than one key indicator.

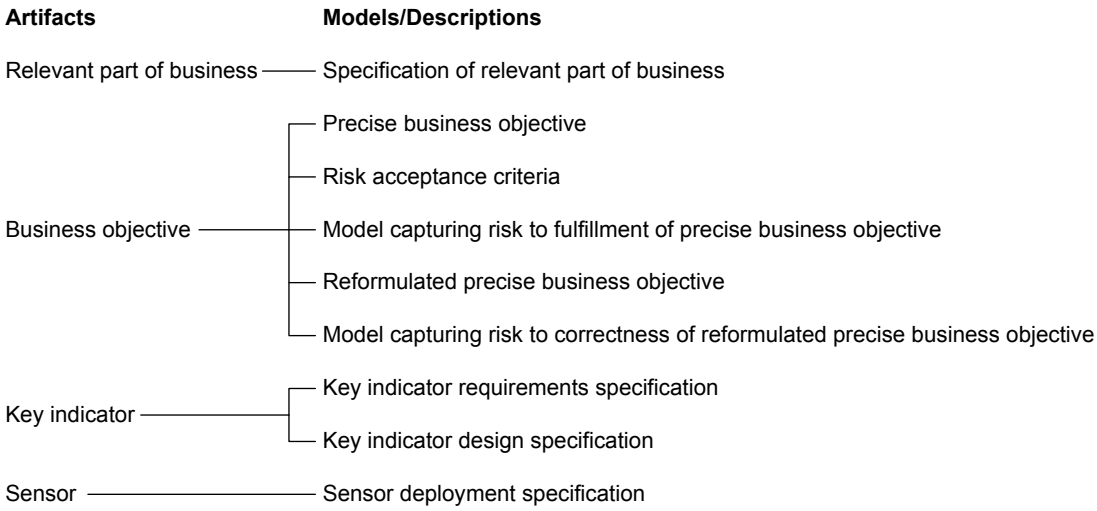

Fig. 2. The models/descriptions developed by ValidKI

B. The models/descriptions developed by ValidKI

As illustrated by Fig. 2, performing the steps of ValidKI results in nine different models/descriptions each of which describes one of the artifacts of Fig. 1 from a certain perspective.

A specification, at a suitable level of abstraction, documents the relevant part of the business in question.

Business objectives are typically expressed at an enterprise level and in such a way that they can easily be understood by for example shareholders, board members, partners, etc. It is therefore often not completely clear what it means to fulfill them. This motivates the need to capture each business objective more precisely.

The fulfillment of a precise business objective may be affected by a number of risks. We therefore conduct a risk analysis to capture risk to the fulfillment of the precise business objective. To evaluate which risks that are acceptable and not acceptable with respect to the fulfillment of the precise business objective, we use risk acceptance criteria. It is the risks that are not acceptable that we need to monitor. The acceptable risks may be thought of to represent uncertainty we can live with. In other words, their potential occurrences are not seen to significantly influence the fulfillment of the business objective.

The degree of fulfillment of a precise business objective is measured by a set of key indicators. To measure its degree of fulfillment there is a need to express each precise business objective in terms of key indicators. We refer to this reformulation as the reformulated precise business objective. Moreover, the correctness of key indicators will be affected if they are not implemented correctly. This may again lead to new unacceptable risks that affect the fulfillment of the precise business objective. Since the reformulated precise business objective is the precise business objective expressed in terms of key indicators, we need to analyze risks to the correctness of the reformulated precise business objective.

The computation of key indicators relies on different kinds of data. To collect the data, sensors need to be deployed in the relevant part of business. Thus, there is a need to specify the deployment of different sensors.

For each key indicator we distinguish between two specifications: the key indicator requirements specification and the key indicator design specification. The first captures requirements to a key indicator with respect to the sensor deployment specifications, while the second defines how the key indicator should be calculated.

C. Validity

ISO/IEC 9126 defines validation as *"confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled"* [7]. Since an indicator is basically a metric that can be compared to a baseline/expected result, the field of metric validation is highly relevant. There is however no agreement upon what constitutes a valid metric [8]. In [8], Meneely et al. present a systematic literature review of papers focusing on validation of software engineering metrics. The literature review began with 2288 papers, which were later reduced to 20 papers. From these 20 papers, the authors extracted and categorized 47 unique validation

Input: A business objective

Step 1: **Establish target**
Step 1.1: Express business objectives more precisely
Step 1.2: Describe relevant part of business

Step 2: **Identify risks to fulfillment of business objective**
Step 2.1: Specify risk acceptance criteria
Step 2.2: Risk identification and estimation
Step 2.3: Risk evaluation

Step 3: **Identify key indicators to monitor risks**
Step 3.1: Deploy sensors to monitor risks
Step 3.2: Specify requirements to key indicators wrt deployed sensors

Step 4: **Evaluate internal validity**
Step 4.1: Express business objective in terms of key indicators
Step 4.2: Evaluate criteria for internal validity

Step 5: **Specify key indicator designs**

Step 6: **Evaluate construct validity**

Output: A set of key indicators and a report arguing its validity with respect to the business objective received as input

Fig. 3. Overview of ValidKI

criteria. The authors argue that metric researchers and developers should select criteria based on the intended usage of the metric. Even though the focus in [8] is on validation of software engineering metrics, a number of the validation criteria presented are general, thus not specific to software engineering. In particular, following [8] we define a set of key indicators to be valid with respect to a business objective if it is valid in the following two ways:

1) **internal validity** – the precise business objective expressed in terms of the key indicators correctly measures the degree to which the business objective is fulfilled; and
2) **construct validity** – the gathering of the sensor measurements of each key indicator is suitable with respect to its requirements specification.

III. Overview of ValidKI

Fig. 3 provides an overview of the ValidKI method. It takes as input a business objective and delivers a set of key indicators and a report arguing its validity with respect to the business objective received as input. When using ValidKI in practice we will typically develop key indicators for a set of business objectives, and not just one which we restrict our attention to here. It should be noticed that when developing key indicators for a set of business objectives, we need to take into account that key indicators (i.e., software or infrastructure) developed for one business objective may affect the validity of key indicators developed for another.

In the following we offer additional explanations for each of the six main steps of the ValidKI method.

A. Establish target

The first main step of ValidKI is all about understanding the target, i.e., understanding exactly what the business objective means and acquiring the necessary understanding of the relevant part of business for which the business objective has been formulated. We distinguish between two sub-steps. In the first sub-step we characterize the business objective more precisely by formulating constraints that need to be fulfilled. In the second sub-step we specify the relevant part of the business.

B. Identify risks to fulfillment of business objective

The second main step of ValidKI is concerned with conducting a risk analysis to identify risks to the fulfillment of the business objective. We distinguish between three sub-steps. In the first sub-step the risk acceptance criteria are

specified. The criteria classify a risk as either acceptable or unacceptable based on its likelihood and consequence. In the second sub-step we identify how threats may initiate risks. We also identify vulnerabilities and threat scenarios leading up to the risks, and we estimate likelihood and consequence. During the risk analysis we may identify risks that pull in the same direction. Such risks should be combined into one risk. The individual risks may be acceptable when considered in isolation, while the combined risk may be unacceptable. In the third sub-step we evaluate the identified risks with respect to the specified risk acceptance criteria.

C. Identify key indicators to monitor risks

The third main step of ValidKI is concerned with identifying key indicators to monitor the unacceptable risks identified in the previous step. We distinguish between two sub-steps. In the first sub-step we specify how sensors should be deployed in the relevant part of business. The key indicators that we identify are to be calculated based on data gathered by the sensors. In the second sub-step we specify our requirements to the key indicators with respect to the deployed sensors. The two sub-steps are typically conducted in parallel.

D. Evaluate internal validity

The fourth main step of ValidKI is concerned with evaluating whether the set of key indicators is internally valid with respect to the business objective. We distinguish between two sub-steps. In the first sub-step we reformulate the precise business objective by expressing it in terms of the identified key indicators. This step serves as an introductory step in the evaluation of internal validity. In the second sub-step we evaluate whether the set of key indicators is internally valid by showing that the reformulated precise business objective from Step 4.1 correctly measures the fulfillment of the precise business objective from Step 1.1.

Internal validity may be decomposed into a broad category of criteria [8]. In the following we list the criteria that we take into consideration. For each criterion, we first provide the definition as given in [8], before we list the papers on which the definition is based.

- **Attribute validity:** *"A metric has attribute validity if the measurements correctly exhibit the attribute that the metric is intending to measure"* [9][10]. In our case, the key indicator needs to correctly exhibit the risk attribute (likelihood or consequence) of the risk that it is measuring. In addition, the key indicator is of little value if it can only produce values that always result in the risk being acceptable or unacceptable.
- **Factor independence:** *"A metric has factor independence if the individual measurements used in the metric formulation are independent of each other"* [11]. This criterion applies especially to composite key indicators that are composed of basic key indicators. A composite key indicator has factor independence if the basic key indicators are independent of each other, i.e., if they do not rely on the same measurements.
- **Internal consistency:** *"A metric has internal consistency if "all of the elementary measurements of a metric are assessing the same construct and are inter-related""* [12]. This criterion also applies especially to composite key indicators that are composed of basic key indicators. If the basic key indicators measure things that are not conceptually related, then the composite key indicator will not have internal consistency. For instance, let us say that we have a composite key indicator that is composed of two basic key indicators. The first basic key indicator measures the code complexity of a software product, while the second measures the cost of shipping the software product to the customers. In this case, the composite key indicator does not have internal consistency, since the two basic key indicators are not conceptually related.
- **Appropriate continuity:** *"A metric has appropriate continuity if the metric is defined (or undefined) for all values according to the attribute being measured"* [10]. An example of a discontinuity is fraction calculations when the denominator is zero. To avoid discontinuity, the key indicator should be defined for that case.
- **Dimensional consistency:** *"A metric has dimensional consistency if the formulation of multiple metrics into a composite metric is performed by a scientifically well-understood mathematical function"* [10][13]. Under dimensional consistency, no information should be lost during the construction of composite key indicators. Loss of information may be experienced if different scales are used for the basic and composite key indicators.
- **Unit validity:** *"A metric has unit validity if the units used are an appropriate means of measuring the attribute"* [10][14]. For instance, the unit fault rate may be used to measure the attribute program correctness [10].

If the set is not internally valid, then we iterate by re-doing Step 3.

E. Specify key indicator designs

In the fifth main step of ValidKI we specify the designs of the identified key indicators. Each design specifies how the key indicator should be calculated. The design also shows how sensors, actors, and different components interact.

F. Evaluate construct validity

In the sixth main step of ValidKI we evaluate whether the set of key indicators has construct validity with respect to the business objective. As with internal validity, construct validity may be decomposed into a broad category of criteria [8]. In the following we list the criteria that we take into consideration. For each criterion, we first provide the definition as given in [8], before we list the papers on which the definition is based.

- **Stability:** *"A metric has stability if it produces the same values "on repeated collections of data under similar circumstances""* [12][15][16]. A key indicator whose calculation involves decisions made by humans, may for example result in different values and thus lack of stability.
- **Instrument validity:** *"A metric has instrument validity if the underlying measurement instrument is valid and properly calibrated"* [10]. In our case, this criterion concerns the sensors that perform the measurements that the key indicator calculations rely on.
- **Definition validity:** *"A metric has definition validity if the metric definition is clear and unambiguous such that its collection can be implemented in a unique, deterministic way"* [11][15][16][17][18]. This criterion concerns the implementation of the key indicators. To implement a key indicator correctly, the key indicator's design specification needs to be clear and unambiguous.

To evaluate the different criteria, we re-do the risk analysis from Step 2.2 with the precise business objective replaced by the reformulated precise business objective, which is the precise business objective expressed in terms of key indicators. For each key indicator we identify risks towards the correctness of the reformulated precise business objective that are the result of threats to criteria for construct validity that the key indicator needs to fulfill. If the risk analysis does not result in any new unacceptable risks, then we have established construct validity for each key indicator. If the set does not have construct validity, then we iterate. We will most likely be re-doing Step 5, but it may also be the case that we need to come up with new key indicators and new sensors. In that case, we re-do Step 3. If the set of key indicators is both internally valid and has construct validity with respect to the business objective, then we have established that the set is valid.

IV. Establish target

In the following we assume that we have been hired to help the public hospital Client H design key indicators to monitor their compliance with Article 8 in the European Convention on Human Rights [19]. The article states the following:

Article 8 – Right to respect for private and family life

1) Everyone has the right to respect for his private and family life, his home and his correspondence.
2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Client H needs to comply with Article 8 since it is a public authority. The consequence for Client H of not complying with Article 8 may be economic loss and damaged reputation. One example [20] of violation of Article 8 is from Finland. A Finnish woman was first treated for HIV at a hospital, before she later started working there as a nurse. While working there she suspected that her co-workers had unlawfully gained access to her medical data. She brought the case to the European Court of Human Rights in Strasbourg which unanimously held that the district health authority responsible for the hospital had violated Article 8 by not protecting the medical data of the woman properly. The district health authority was held liable to pay damages to the woman. Client H has therefore established the following business objective:

Business objective BO-A8: Client H complies with Article 8 in the European Convention on Human Rights.

Client H wants to make use of key indicators to monitor the degree of fulfillment of BO-A8, and now they have hired us to use ValidKI to design them. In the rest of this section we conduct Step 1 of ValidKI on behalf of Client H with respect to BO-A8.

A. Express business objectives more precisely (Step 1.1 of ValidKI)

Article 8 states under which circumstances a public authority can interfere with someone's right to privacy. One of these circumstances is *"for the protection of health,"* which is what Client H wants us to focus on. In the context of Client H this means to provide medical assistance to patients. The ones who provide this assistance are the health-care professionals of Client H.

The medical history of a patient is regarded as both sensitive and private. At Client H, the medical history of a patient is stored in an electronic patient record (EPR). An EPR is *"an electronically managed and stored collection or collocation of recorded/registered information on a patient in connection with medical assistance"* [21]. The main purpose of an EPR is to communicate information between health-care professionals that provide medical care to a patient. To protect the privacy of its patients, Client H restricts the use of EPRs. In order to comply with Article 8, Client H allows a health-care professional to interfere with the privacy of a patient only when providing medical assistance to this patient. Hence, the dealing with EPRs within the realms of Client H is essential.

For Client H it is important that every access to information in an EPR is in accordance with Article 8. A health-care professional should only access a patient's EPR if he/she provides medical assistance to that patient, and he/she should only access information that is necessary for providing the medical assistance. The information accessed can not be used for any other purpose than providing medical assistance to patients. Accesses to information in EPRs not needed for providing medical assistance would not be in accordance with Article 8. Also, employees that are not health-care professionals and work within the jurisdiction of Client H are not allowed to access EPRs. Based on the constraints provided by Client H, we decide to express BO-A8 more precisely as follows:

Precise business objective PBO-A8: $C_1 \wedge C_2 \wedge C_3$

- **Constraint C_1:** Health-care professionals acting on behalf of Client H access:
  - a patient's EPR only when providing medical assistance to that patient
  - only the information in a patient's EPR that is necessary for providing medical assistance to that patient
- **Constraint C_2:** Health-care professionals acting on behalf of Client H do not use the information obtained from a patient's EPR for any other purpose than providing medical assistance to that patient.
- **Constraint C_3:** Employees that are not health-care professionals and that work within the jurisdiction of Client H do not access EPRs.

As indicated by PBO-A8's definition, all three constraints must be fulfilled in order for PBO-A8 to be fulfilled.

B. Describe relevant part of business (Step 1.2 of ValidKI)

To design key indicators to monitor BO-A8 we need to understand the part of business that is to comply with BO-A8 and therefore is to be monitored. "Public hospital *Client H*" has outsourced some of its medical services to two private hospitals. These two are referred to as "Private hospital *X-ray*" and "Private hospital *Blood test analysis*" in Fig. 4. The first hospital does all the X-ray work for Client H, while the second hospital does all the blood test analyses. Client H is not only responsible for its own handling of EPRs, but also the outsourcing partners' handling of EPRs, when they act on behalf of Client H.

In Fig. 4, the rectangles inside and outside the gray containers represent systems/actors, while the arrows in the figure represent the exchange of data between different systems/actors. In the figure, we only show some of the rectangles and arrows that should be part of the gray containers of "Public hospital *Client H*" and "Private hospital *Blood test analysis*." All the rectangles and arrows with names in italic that are part of the gray container of "Private hospital *X-ray*" should also be part of the gray containers of "Public hospital *Client H*" and "Private hospital *Blood test analysis*."

As can be seen in Fig. 4, Client H outsources medical tasks to the two private hospitals, and gets in return the results from performing these tasks. All three health-care institutions employs some kind of EPR system for

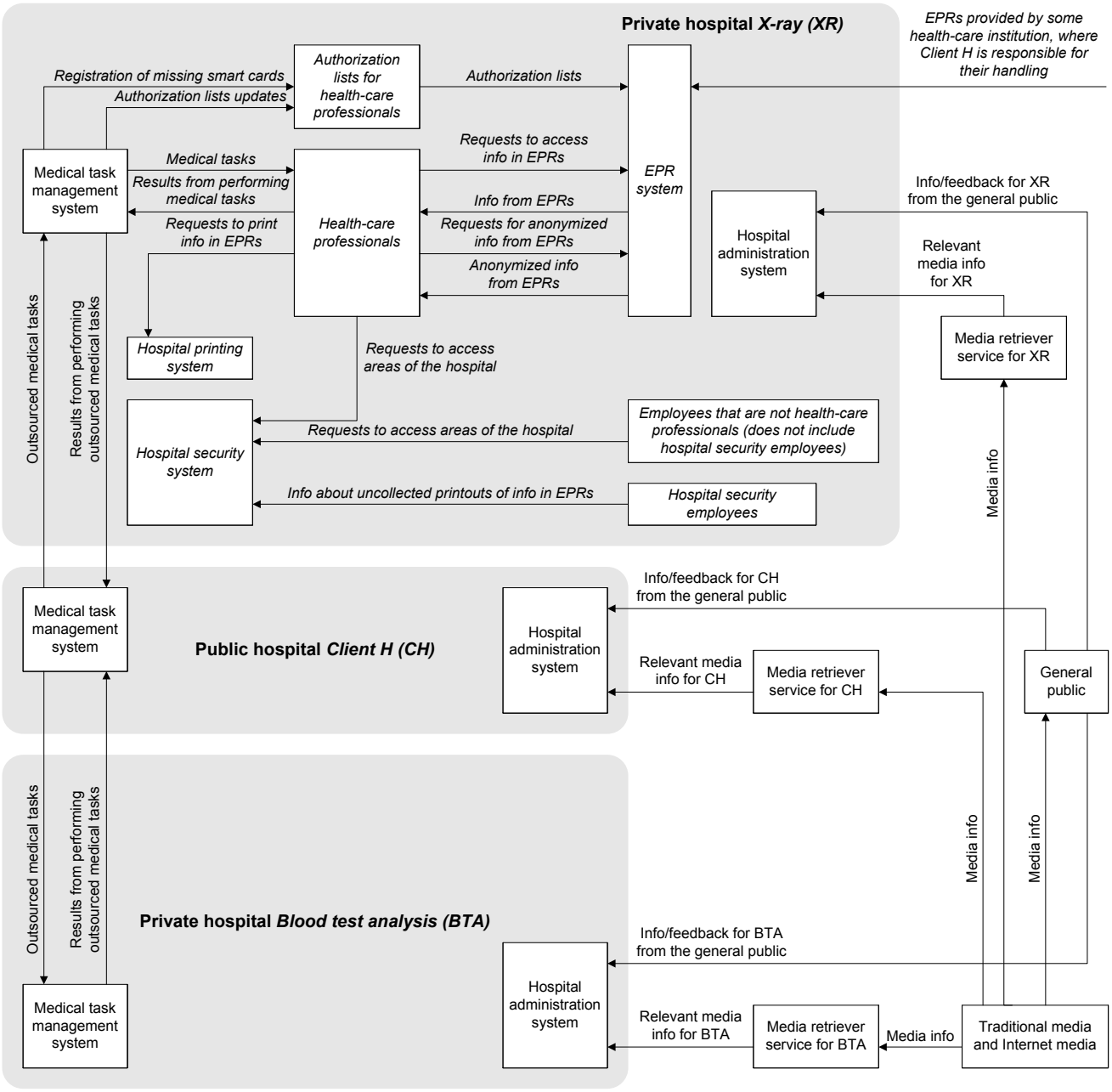

Fig. 4. Specification of relevant part of business

handling the EPRs. An EPR system is *"an electronic system with the necessary functionality to record, retrieve, present, communicate, edit, correct, and delete information in electronic patient records"* [21]. These systems use EPRs provided by different health-care institutions. As shown in Fig. 4, these systems are only of interest when they handle EPRs where Client H is responsible for their handling.

At the three health-care institutions, most of the medical tasks that a health-care professional conducts during a working day are known in advance. It is known which patients the professional will treat and what kind of information the professional will need access to in order to treat the different patients. Client H and the two outsourcing partners maintain for each health-care professional an authorization list documenting which patients the professional is treating and what kind of information the professional needs for this purpose. These lists are used by the EPR systems and they are updated on a daily basis by the medical task management systems. Many of these updates are automatic. For instance, when Client H is assigned a new patient, then this patient is added to the lists of the health-care professionals who will be treating this patient.

Each EPR is owned by a patient, which is natural since the information stored in the EPR is about the patient in question. As already mentioned, the content of a patient's EPR is both considered sensitive and private. Moreover, some of the EPRs may contain information that is considered highly sensitive and private. Such information may for instance describe medical treatment received by a patient in relation to:

- the patient being the victim of a crime (e.g., rape, violence, etc.);
- sexual transferable diseases or abortion; and
- mortal or infectious mortal diseases.

Information classified as highly sensitive and private is handled with even more care than information that is just classified as sensitive and private. To raise awareness of the criticality of such information and to enable monitoring of its use, the EPR systems at the three health-care institutions tag highly sensitive and private information in EPRs based on predefined rules.

Accesses to information in EPRs can be classified as *authorized* or *unauthorized* based on the authorization lists of health-care professionals. An access is classified as authorized if the professional needs the information to do a planned task. Otherwise, the access is classified as unauthorized. If an access is classified as unauthorized then it is possible to check in retrospect whether the access was necessary. In an emergency situation, for instance when a patient is having a heart attack, a health-care professional often needs access to information in an EPR that he/she was not supposed to access. By checking in retrospect whether unauthorized accesses were necessary it is possible to classify the unauthorized accesses into two groups; one for accesses that were necessary, and one for those that were not. The first group is called *approved* unauthorized accesses, while the second group is called *not approved* unauthorized accesses. All accesses that are classified as not approved unauthorized accesses are considered as *illegal* accesses.

At Client H and the two outsourcing partners, health-care professionals use smart cards for accessing information in EPRs. If a card is lost or stolen, the owner must report it as missing, since missing cards may be used by other health-care professionals or others to access EPRs illegally. When the card has been registered as missing it can no longer be used. When reporting it as missing, the last time the card owner used it before noticing that it was missing is recorded. All accesses to EPRs that have occurred between this time and the time it was registered as missing are considered as illegal accesses.

At the three hospitals, the doors into the different areas are fitted with smart card locks. In order to open a door, an employee needs to insert his/hers smart card into the lock. A security system is used by each hospital to allow or deny an employee access to a specific area based on the employee's access credentials. Moreover, health-care professionals often need to print information in EPRs. Each hospital relies on a printing system to achieve this. This system issues the different print jobs to printers located in rooms with doors fitted with smart card locks. Since each printer is used by a number of employees, the three hospitals run the risk of printed information being disclosed to other employees if the employee responsible for the print job forgets to collect his/hers printout. To minimize this risk, each hospital has security employees that collect uncollected printouts of information from EPRs at the different printers on a regular basis. Each printer at the three hospitals annotates each printout with the date and time it was printed, as well as an ID for the employee that issued the print job. A security employee removes a printout of sensitive and private information from an EPR if it has been laying on the printer for 30 minutes or more, while he/she removes a printout of highly sensitive and private information if it has been laying on the printer for 15 minutes or more. For each removed printout, the health-care professional that issued the print job is notified about the removal and asked to collect the printout at the security office at the hospital in question.

A health-care professional relies from time to time on information obtained from patients' EPRs for other purposes than providing medical assistance to the patients in question. The information may be needed for the purpose of providing medical assistance to another patient, or it may be needed in research projects. To support these tasks, the three hospitals have made it possible for health-care professionals to obtain anonymized information from EPRs, i.e., information that cannot be linked to specific patients. It should be noticed that health-care professionals need to obtain specific permissions to obtain and use anonymized information from EPRs.

At each of the three hospitals, a media retriever service is used to collect relevant information from the traditional media (newspapers, TV, radio, etc.) and the Internet media (Internet newspapers, etc.). The three hospitals also encourage the general public to provide feedback on how satisfied they are with the hospitals' services. The general public also serves another purpose for the three hospitals. The media retriever services can only to a limited extent retrieve information from social media (Facebook, Twitter, etc.) and Internet forums. The three hospitals therefore

TABLE I
CONSEQUENCE SCALE FOR THE ASSET "FULFILLMENT OF PBO-A8" (TOP) AND LIKELIHOOD SCALE (BOTTOM)

Consequence	**Description**
Catastrophic	Law enforcement agencies penalize Client H after having been notified about the incident
Major	Health authorities penalize Client H after having been notified about the incident
Moderate	Health authorities are notified about the incident
Minor	Head of hospital is notified about the incident
Insignificant	Head of department is notified about the incident
Likelihood	**Description**
Certain	Five times or more per year $[50, \infty\rangle$: 10 years
Likely	Two to five times per year $[20, 49]$: 10 years
Possible	Once a year $[6, 19]$: 10 years
Unlikely	Less than once per year $[2, 5]$: 10 years
Rare	Less than once per ten years $[0, 1]$: 10 years

TABLE II
RISK EVALUATION MATRIX FOR THE ASSET "FULFILLMENT OF PBO-A8"

Consequence / **Likelihood**	Insignificant	Minor	Moderate	Major	Catastrophic
Rare					
Unlikely					
Possible					
Likely					
Certain					

encourage the general public to notify them about information found in social media or on Internet forums that may be of relevance. A person of the general public is awarded if the information is very relevant. The information provided by the media retriever services and the general public is first and foremost used by the hospitals to assess how they are perceived by the public. Sometimes, however, the collected information may indicate or reveal that information from EPRs have been leaked to the public.

V. IDENTIFY RISKS TO FULFILLMENT OF BUSINESS OBJECTIVE

A. Specify risk acceptance criteria (Step 2.1 of ValidKI)

Before we specify the risk acceptance criteria, we need to establish scales for measuring likelihood and consequence. Table I presents these scales. We view "Fulfillment of PBO-A8" as the asset to be protected. In Table II the risk acceptance criteria for the asset "Fulfillment of PBO-A8" are expressed in terms of a risk evaluation matrix. Risks whose values belong to the white area of the matrix are acceptable, while risks whose values belong to the gray area are unacceptable.

B. Risk identification and estimation (Step 2.2 of ValidKI)

Based on the information provided by the representatives of Client H, we identify and estimate risk. For this purpose we use the CORAS methodology [22]. However, other approaches to risk analysis may be used instead. Using CORAS we identify how threats may initiate risks that harm the asset "Fulfillment of PBO-A8" if they occur.

The CORAS threat diagram in Fig. 5 provides a high-level overview of how the fulfillment of the precise business objective PBO-A8 may be harmed. The threat diagram contains four referring threat scenarios that refer to the referenced threat scenarios in Figs. 6 – 9. We refer to i_x and o_y of the referring threat scenarios as in-gate and out-gate, respectively. Relations to an element inside a referenced threat scenario must go through an in-gate, while relations to an element outside the referenced threat scenario must go through an out-gate. The likelihood value of an in-gate i_x documents the contribution of an element outside the referenced threat scenario via gate i_x to the

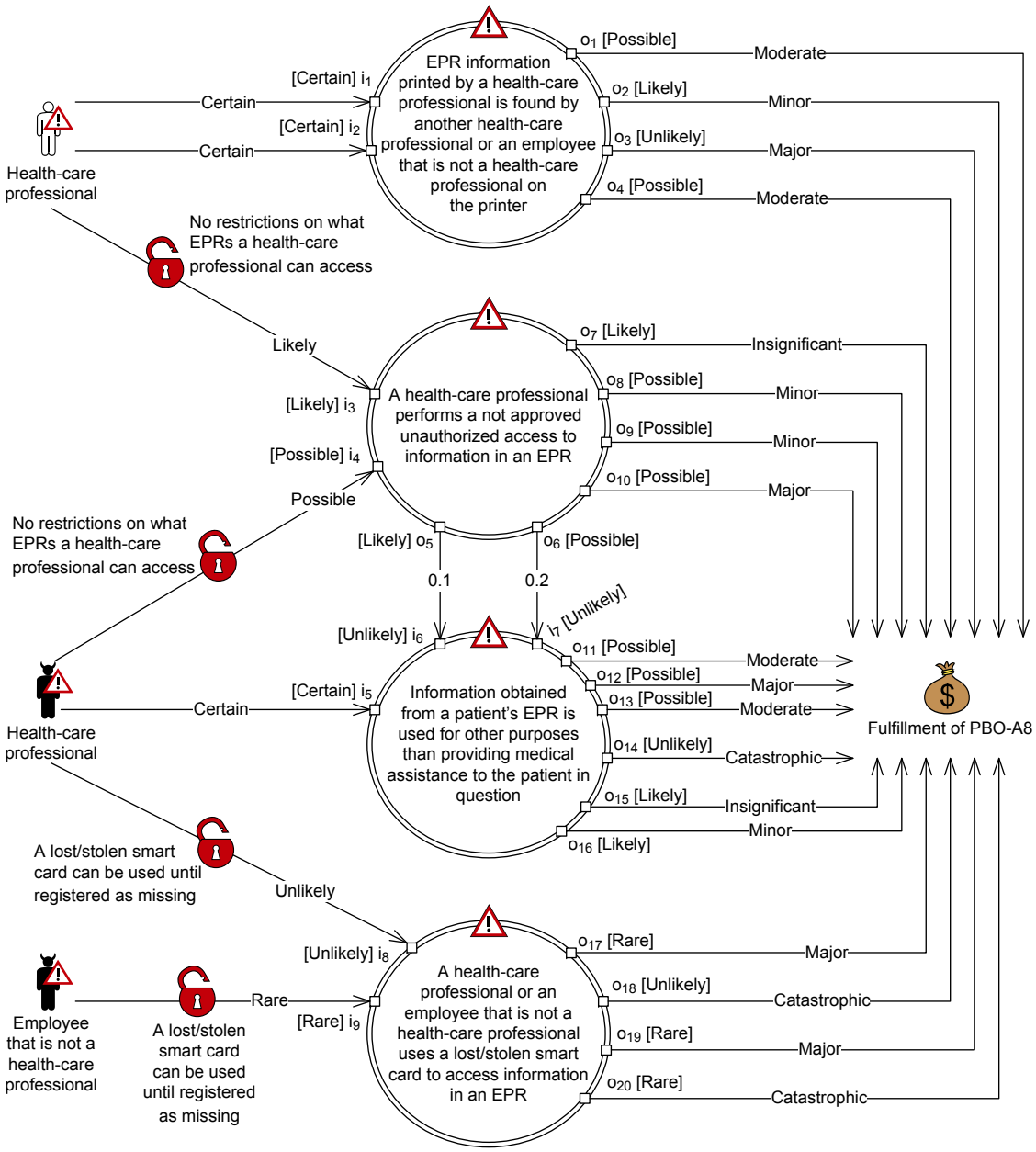

Fig. 5. CORAS threat diagram providing a high-level overview of the results from the risk identification and estimation

likelihood of an element inside the referenced threat scenario, while the likelihood of the out-gate o_y documents the contribution of the likelihood of an element inside the referenced threat scenario via gate o_y to the likelihood of an element outside the referenced threat scenario.

The CORAS threat diagram in Fig. 5 contains three human threats; one accidental (the white one) and two deliberate (the black ones). The accidental human threat "Health-care professional" may initiate the threat scenario "Unauthorized access to information in a patient's EPR" in the referenced threat scenario "A health-care professional performs a not approved unauthorized access to information in an EPR" in Fig. 7 via the in-gate i_3 with likelihood "Likely" by exploiting the vulnerability "No restrictions on what EPRs a health-care professional can access." We can also see that the deliberate human threat "Health-care professional" may initiate this threat scenario via the in-gate i_4 with likelihood "Possible" by exploiting the same vulnerability, and that the threat scenario occurs with likelihood "Certain." If the threat scenario in Fig. 7 occurs then it leads to the threat scenario "Unauthorized access to sensitive and private information" in the same figure with conditional likelihood "0.7." This threat scenario leads to the risk "R5: Not approved unauthorized access to sensitive and private information in an EPR, where the owner

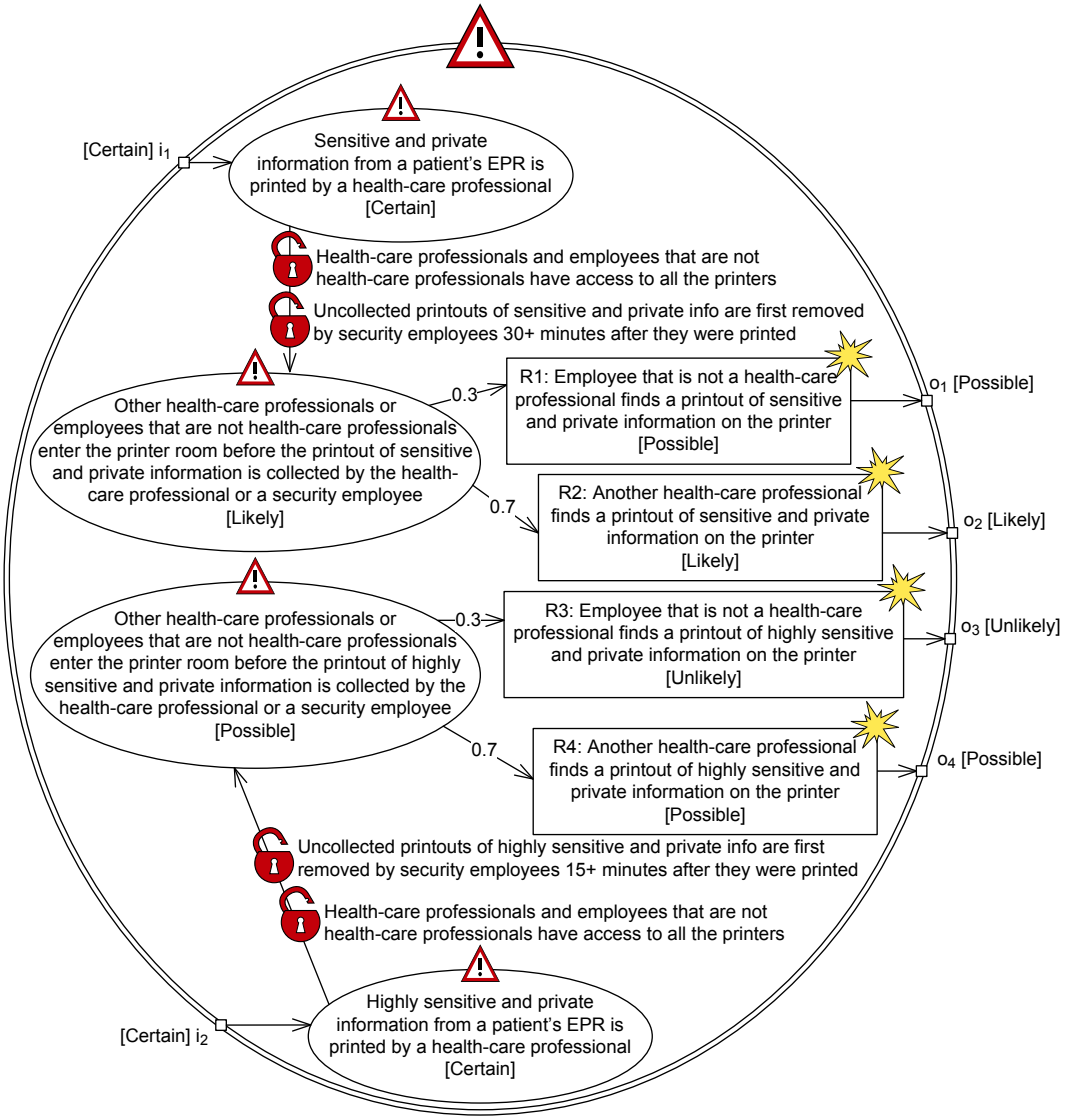

Fig. 6. The referenced threat scenario "EPR information printed by a health-care professional is found by another health-care professional or an employee that is not a health-care professional on the printer," referred to in Fig. 5

of the EPR is a patient of the accessor" with conditional likelihood "0.6" if it occurs. The risk occurs with likelihood "Likely." As can be seen in Figs. 5 and 7, the risk impacts the asset "Fulfillment of PBO-A8" via the out-gate o_7 with consequence "Insignificant" if it occurs.

The referenced threat scenarios in Figs. 6 – 9 document risks that affect the fulfillment of the constraints referred to in the precise business objective PBO-A8. The risks $R2$, $R4$, $R5$ – $R8$, $R15$, and $R16$ affect the fulfillment of constraint C_1, while the risks $R9$ – $R14$ affect the fulfillment of constraint C_2. Moreover, the risks $R1$, $R3$, $R17$, and $R18$ affect the fulfillment of constraint C_3. Notice that in the referenced threat scenario in Fig. 7, we distinguish between not approved unauthorized accesses to information in EPRs where the owner of the EPR is a patient and not a patient of the accessor. Client H finds it most serious if the owner of the EPR is not a patient of the accessor. We also distinguish between not approved unauthorized accesses to sensitive and private information and not approved unauthorized accesses to highly sensitive and private information. Naturally, Client H finds not approved unauthorized accesses to the latter type of information the most serious.

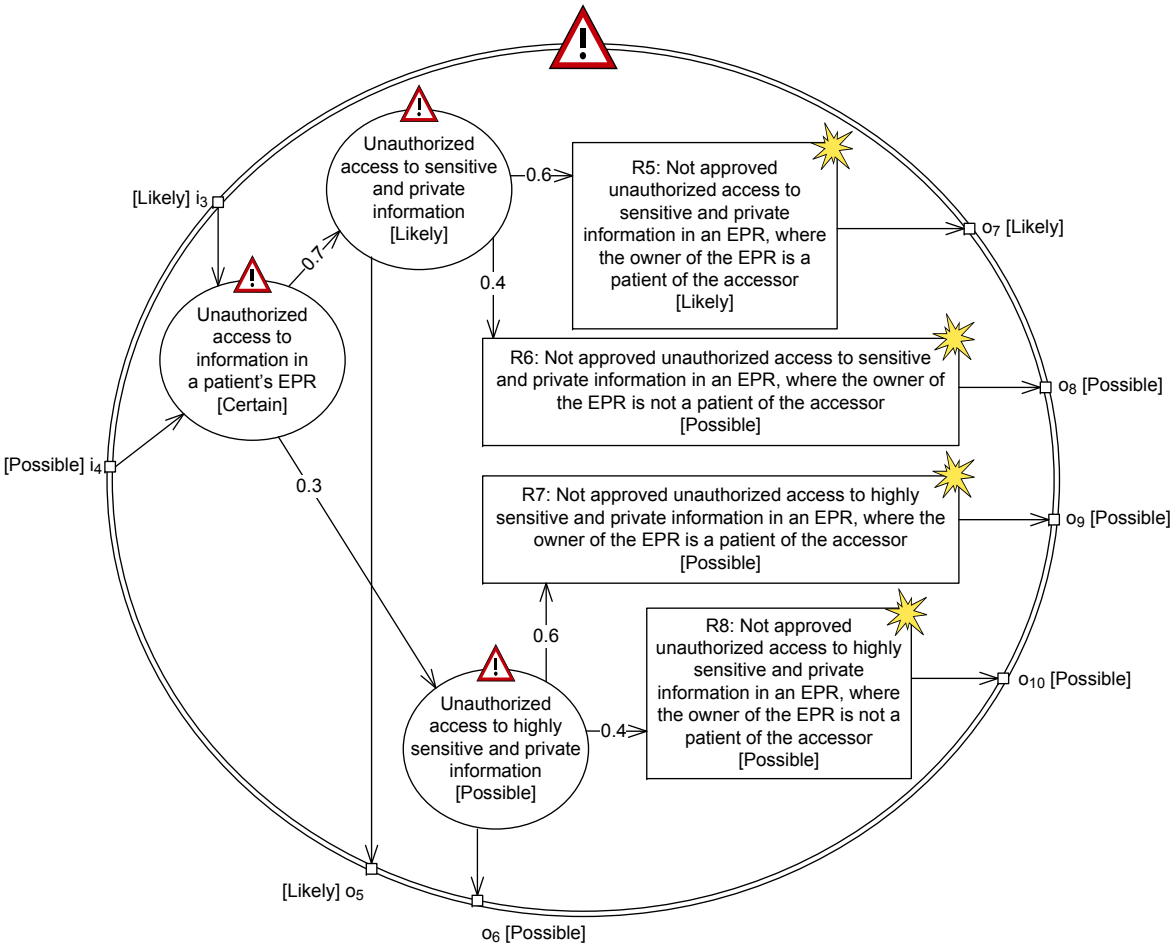

Fig. 7. The referenced threat scenario "A health-care professional performs a not approved unauthorized access to information in an EPR," referred to in Fig. 5

TABLE III
THE RISK EVALUATION MATRIX FROM TABLE II WITH THE ACCEPTABLE AND UNACCEPTABLE RISKS INSERTED

Consequence / **Likelihood**	Insignificant	Minor	Moderate	Major	Catastrophic
Rare				$R15$, $R17$	$R18$
Unlikely				$R3$	$R12$, $R16$
Possible		$R6$, $R7$	$R1$, $R4$, $R9$, $R11$	$R8$, $R10$	
Likely	$R5$, $R13$	$R2$, $R14$			
Certain					

C. Risk evaluation (Step 2.3 of ValidKI)

The risk evaluation consists in plotting the risks into the risk evaluation matrix according to their likelihoods and consequences. As indicated in Table III, four out of the 18 risks namely $R8$, $R10$, $R12$, and $R16$ are unacceptable with respect to the fulfillment of the precise business objective PBO-A8.

During the risk evaluation, we also decide that some of the risks need to be accumulated since they pull in the same direction. We decide to accumulate the following risks: $R1$ and $R2$; $R3$ and $R4$; $R15$ and $R17$; and $R16$ and $R18$. All of these risks, with the exception of $R18$, are acceptable when considered in isolation. Risks are accumulated by accumulating their likelihood and consequence values. We accumulate the risks as follows:

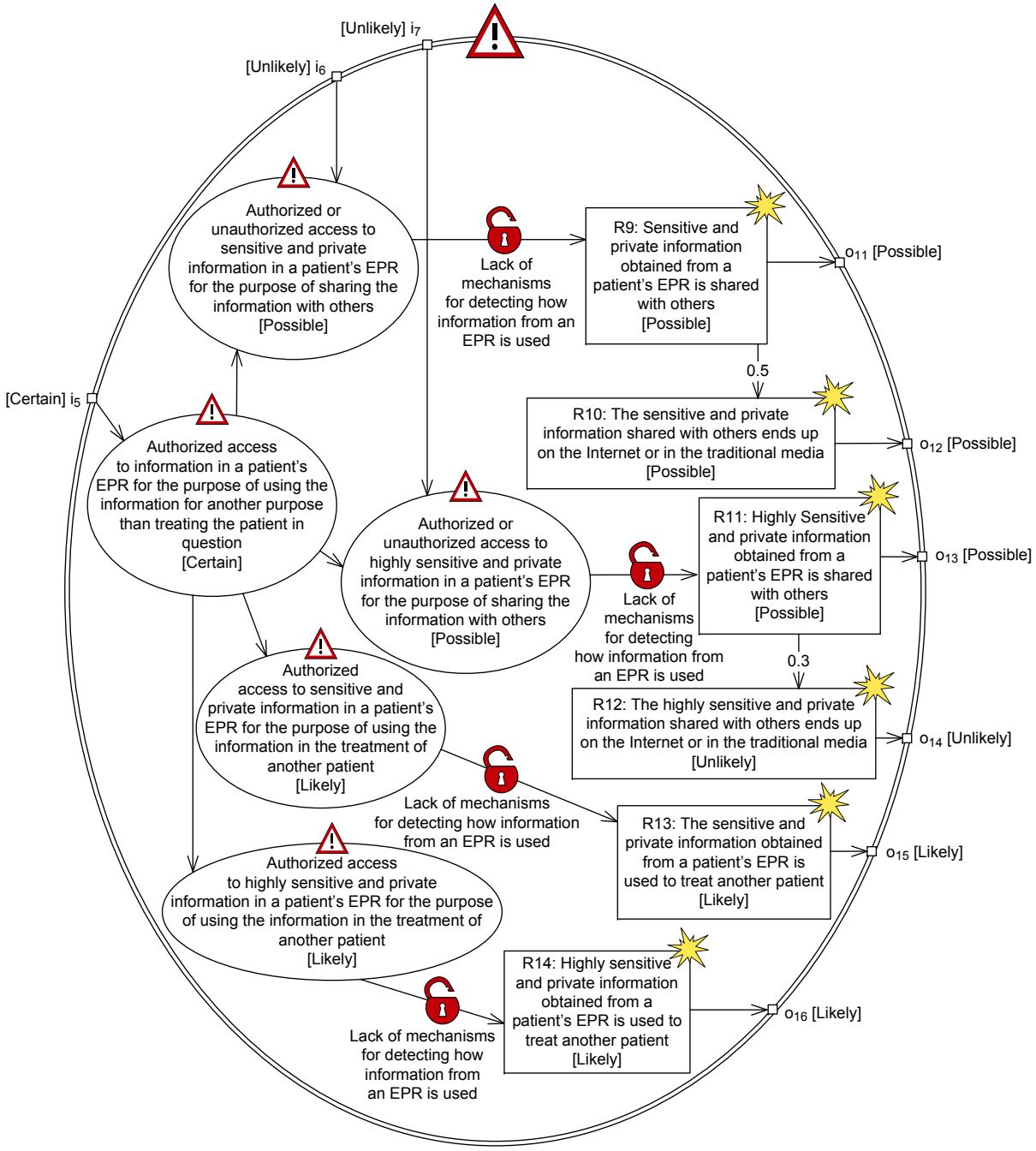

Fig. 8. The referenced threat scenario "Information obtained from a patient's EPR is used for other purposes than providing medical assistance to the patient in question," referred to in Fig. 5

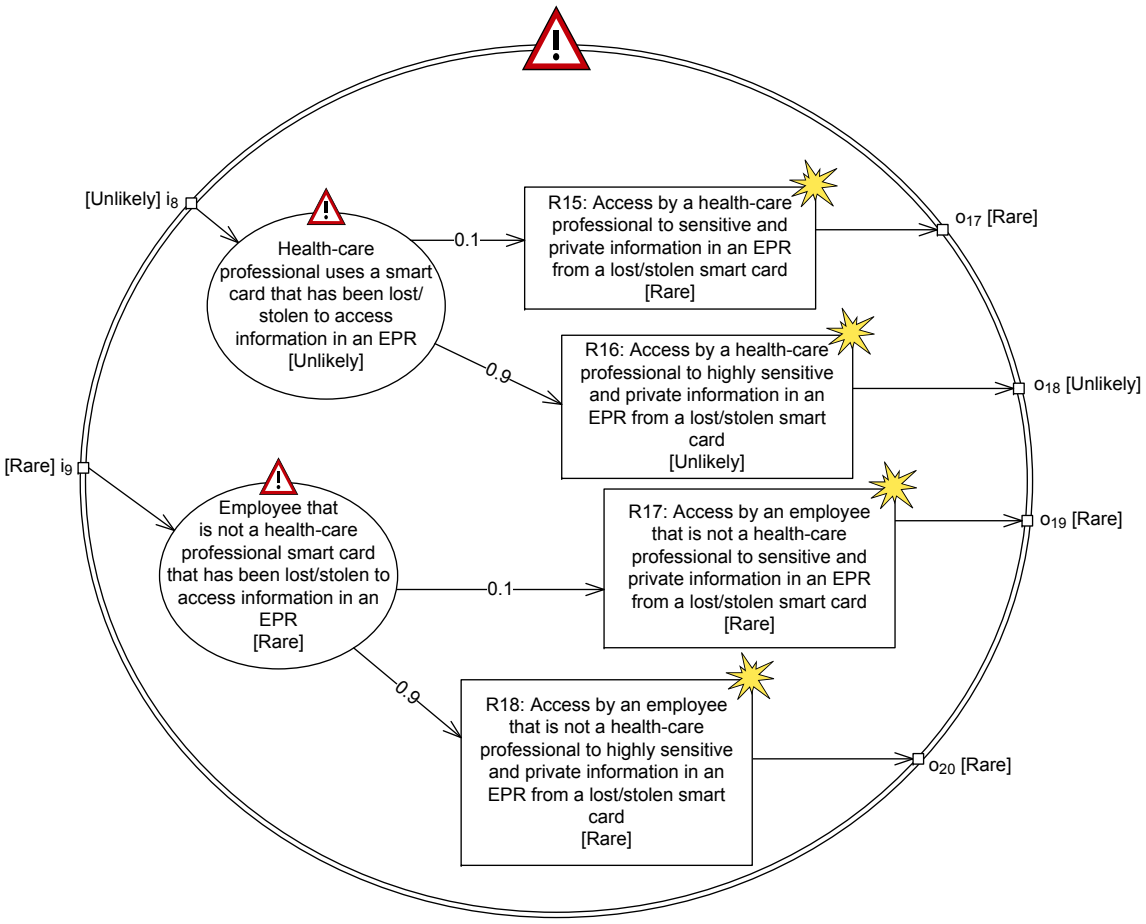

Fig. 9. The referenced threat scenario "A health-care professional or an employee that is not a health-care professional uses a lost/stolen smart card to access information in an EPR," referred to in Fig. 5

- The accumulated risk "$R1\&R2$: Another health-care professional or employee that is not a health-care professional finds a printout of sensitive and private information on the printer." It occurs with likelihood "Likely" and it impacts the asset with consequence "Moderate." The accumulated risk is based on:
  - The risk $R1$ which occurs with likelihood "Possible," while it impacts the asset with consequence "Moderate."
  - The risk $R2$ which occurs with likelihood "Likely," while it impacts the asset with consequence "Minor."
- The accumulated risk "$R3\&R4$: Another health-care professional or employee that is not a health-care professional finds a printout of highly sensitive and private information on the printer." It occurs with likelihood "Possible" and it impacts the asset with consequence "Major." The accumulated risk is based on:
  - The risk $R3$ which occurs with likelihood "Unlikely," while it impacts the asset with consequence "Major."
  - The risk $R4$ which occurs with likelihood "Possible," while it impacts the asset with consequence "Moderate."
- The accumulated risk "$R15\&R17$: Access by a health-care professional or an employee that is not a health-care professional to sensitive and private information in an EPR from a lost/stolen smart card." It occurs with likelihood "Rare" and it impacts the asset with consequence "Major." The accumulated risk is based on:
  - The risk $R15$ which occurs with likelihood "Rare," while it impacts the asset with consequence "Major."
  - The risk $R17$ which occurs with likelihood "Rare," while it impacts the asset with consequence "Major."
- The accumulated risk "$R16\&R18$: Access by a health-care professional or an employee that is not a health-care professional to highly sensitive and private information in an EPR from a lost/stolen smart card." It occurs

TABLE IV
THE RISK EVALUATION MATRIX FROM TABLE III AFTER RISKS HAVE BEEN ACCUMULATED

Likelihood \ Consequence	Insignificant	Minor	Moderate	Major	Catastrophic
Rare				$R15\&R17$	
Unlikely					$R12$, $R16\&R18$
Possible		$R6$, $R7$	$R9$, $R11$	$R3\&R4$, $R8$, $R10$	
Likely	$R13$	$R5$, $R14$	$R1\&R2$		
Certain					

with likelihood "Unlikely" and it impacts the asset with consequence "Catastrophic." The accumulated risk is based on:

- The risk $R16$ which occurs with likelihood "Unlikely," while it impacts the asset with consequence "Catastrophic."
- The risk $R18$ which occurs with likelihood "Rare," while it impacts the asset with consequence "Catastrophic."

Since we are operating with a coarse-grained likelihood scale with intervals, we find it sufficient to do a rough aggregation of the likelihoods in order to determine to which likelihood interval the different accumulated risks belong. For the accumulated risk $R15\&R17$ we end up with the likelihood "Rare," while for each of the other accumulated risks, we end up with an aggregated likelihood that gravitates towards the highest of the two likelihoods. We therefore decide to use the highest likelihood to represent the accumulated likelihood in each of these cases. Moreover, we accumulate consequences by taking the average. In all of the cases where the two consequence values differ, we end up with an average that gravitates towards the highest consequence value. We therefore find it suitable to use the highest consequence value to represent the accumulated consequence in each of these cases.

In Table IV we have plotted the accumulated risks according to their likelihoods and consequences. As we can see from the table, all the accumulated risks with the exception of $R15\&R17$ are unacceptable. Table IV shows that the risks $R1\&R2$, $R3\&R4$, $R8$, $R10$, $R12$, and $R16\&R18$ are unacceptable with respect to the fulfillment of the precise business objective PBO-A8.

VI. IDENTIFY KEY INDICATORS TO MONITOR RISKS

A. Deploy sensors to monitor risks (Step 3.1 of ValidKI)

Fig. 10, which is a detailing of the target description in Fig. 4, specifies the deployment of sensors in the relevant part of business. This specification corresponds to the sensor deployment specification referred to in Fig. 2. An antenna-like symbol is used to represent each sensor in Fig. 10. The different sensors monitor data messages exchanged within the relevant part of business. The results from the monitoring are to be used in the calculation of key indicators.

In Fig. 10, sensor deployments are only shown for "Private hospital *X-ray*." It should be noticed that "Public hospital *Client H*" and "Private hospital *Blood test analysis*" will have the same sensors as "Private hospital *X-ray*." The following sensors are deployed in the relevant part of business:

- $S_{\text{CH-REG-MIS-SC}}$, $S_{\text{BTA-REG-MIS-SC}}$, and $S_{\text{XR-REG-MIS-SC}}$ monitor data messages related to the registration of missing smart cards at Client H, Blood test analysis, and X-ray, respectively.
- $S_{\text{CH-AUTH-LIST}}$, $S_{\text{BTA-AUTH-LIST}}$, and $S_{\text{XR-AUTH-LIST}}$ monitor data messages related to the authorization lists employed by the EPR systems at Client H, Blood test analysis, and X-ray, respectively.
- $S_{\text{CH-ACC-INFO-EPR}}$, $S_{\text{BTA-ACC-INFO-EPR}}$, and $S_{\text{XR-ACC-INFO-EPR}}$ monitor data messages where each message is a request issued by health-care professional to access information in an EPR at Client H, Blood test analysis, and X-ray, respectively. It is not necessary to monitor the actual information received, since health-care professionals will always get the information they request.
- $S_{\text{CH-INFO-GP}}$, $S_{\text{BTA-INFO-GP}}$, and $S_{\text{XR-INFO-GP}}$ monitor data messages where each message contains info/feedback from the general public for Client H, Blood test analysis, and X-ray, respectively.

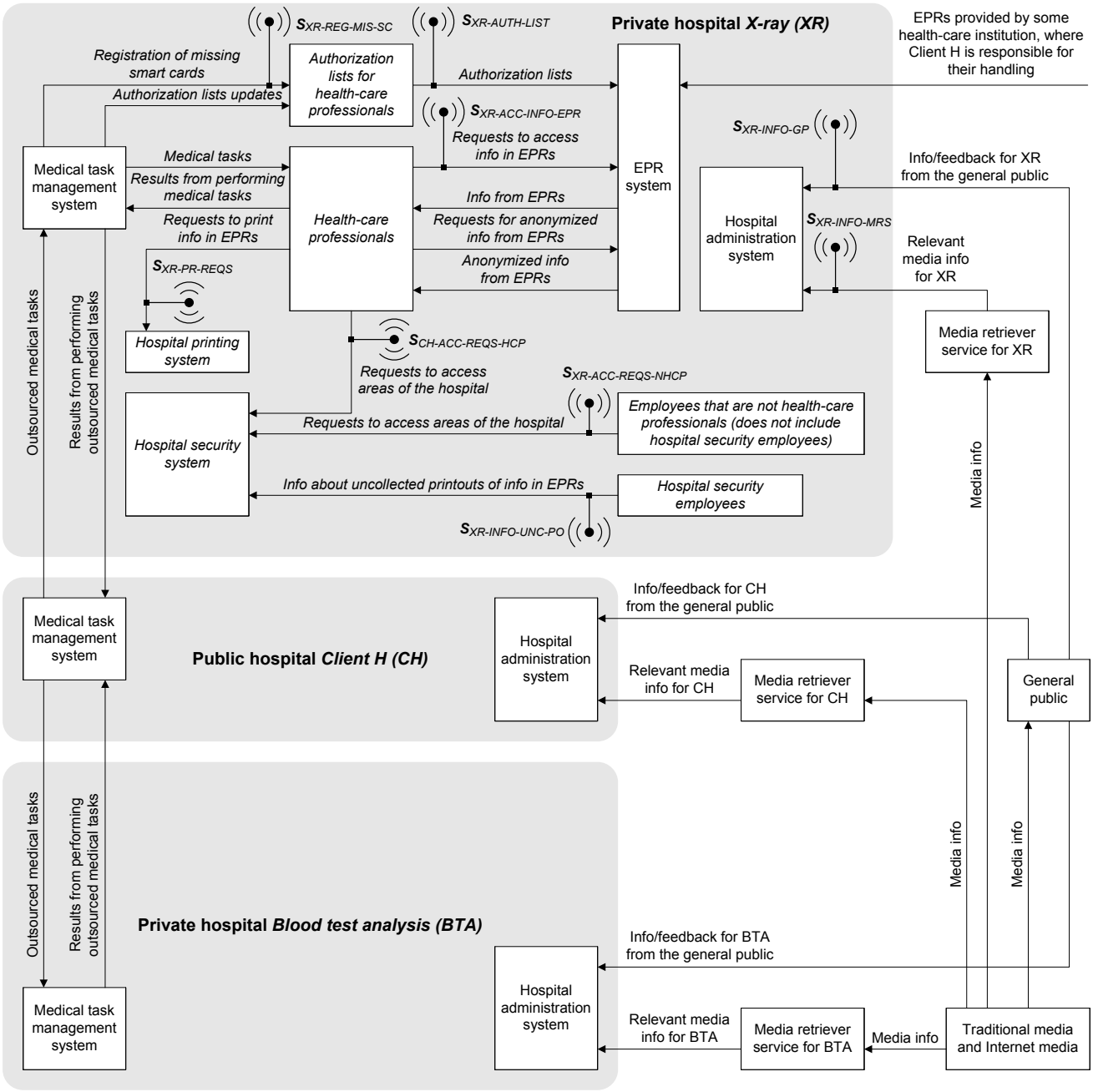

Fig. 10. Deployment of sensors in the relevant part of business

- $S_{\text{CH-INFO-MRS}}$, $S_{\text{BTA-INFO-MRS}}$, and $S_{\text{XR-INFO-MRS}}$ monitor data messages where each message contains relevant information collected by media retriever services from the traditional media or the Internet for Client H, Blood test analysis, and X-ray, respectively.
- $S_{\text{CH-PR-REQS}}$, $S_{\text{BTA-PR-REQS}}$, and $S_{\text{XR-PR-REQS}}$ monitor data messages related to printing of information in EPRs by health-care professionals at Client H, Blood test analysis, and X-ray, respectively.
- $S_{\text{CH-ACC-REQS-HCP}}$, $S_{\text{BTA-ACC-REQS-HCP}}$, and $S_{\text{XR-ACC-REQS-HCP}}$ monitor data messages related to area access requests issued by health-care professionals at Client H, Blood test analysis, and X-ray, respectively.
- $S_{\text{CH-ACC-REQS-NHCP}}$, $S_{\text{BTA-ACC-REQS-NHCP}}$, and $S_{\text{XR-ACC-REQS-NHCP}}$ monitor data messages related to area access requests issued by employees that are not health-care professionals at Client H, Blood test analysis, and X-ray, respectively.
- $S_{\text{CH-INFO-UNC-PO}}$, $S_{\text{BTA-INFO-UNC-PO}}$, and $S_{\text{XR-INFO-UNC-PO}}$ monitor data messages related to registrations of uncol-

TABLE V
KEY INDICATOR REQUIREMENTS SPECIFICATIONS FOR THE COMPOSITE KEY INDICATOR $K_{\text{PR-SP-EPR-INFO}}$ AND THE BASIC KEY INDICATORS $K_{\text{CH-PR-SP-EPR-INFO}}$, $K_{\text{BTA-PR-SP-EPR-INFO}}$, AND $K_{\text{XR-PR-SP-EPR-INFO}}$

Requirements for $K_{\text{X-PR-SP-EPR-INFO}}$, where $X \in \{\text{CH}, \text{BTA}, \text{XR}\}$	
In:	$S_{\text{X-ACC-REQS-NHCP}}, S_{\text{X-ACC-REQS-HCP}}, S_{\text{X-PR-REQS}}, S_{\text{X-INFO-UNC-PO}} : M^*$
Out:	$K_{\text{X-PR-SP-EPR-INFO}} : \mathbb{R}$
Description:	$K_{\text{X-PR-SP-EPR-INFO}}$ = "The number of times since the monitoring started that health-care professionals or employees that are not health-care professionals have found printouts of sensitive and private information from EPRs on printers at X"

Requirements for $K_{\text{PR-SP-EPR-INFO}}$	
In:	$S_{\text{CH-ACC-REQS-NHCP}}, S_{\text{BTA-ACC-REQS-NHCP}}, S_{\text{XR-ACC-REQS-NHCP}} : M^*$ $S_{\text{CH-ACC-REQS-HCP}}, S_{\text{BTA-ACC-REQS-HCP}}, S_{\text{XR-ACC-REQS-HCP}} : M^*$ $S_{\text{CH-PR-REQS}}, S_{\text{BTA-PR-REQS}}, S_{\text{XR-PR-REQS}} : M^*$ $S_{\text{CH-INFO-UNC-PO}}, S_{\text{BTA-INFO-UNC-PO}}, S_{\text{XR-INFO-UNC-PO}} : M^*$
Out:	$K_{\text{PR-SP-EPR-INFO}} : \mathbb{R}$
Description:	$K_{\text{PR-SP-EPR-INFO}} = \frac{10 \cdot (K_{\text{CH-PR-SP-EPR-INFO}} + K_{\text{BTA-PR-SP-EPR-INFO}} + K_{\text{XR-PR-SP-EPR-INFO}})}{\textit{Number of years since the monitoring started}}$

TABLE VI
KEY INDICATOR REQUIREMENTS SPECIFICATIONS FOR THE COMPOSITE KEY INDICATOR $K_{\text{PR-HSP-EPR-INFO}}$ AND THE BASIC KEY INDICATORS $K_{\text{CH-PR-HSP-EPR-INFO}}$, $K_{\text{BTA-PR-HSP-EPR-INFO}}$, AND $K_{\text{XR-PR-HSP-EPR-INFO}}$

Requirements for $K_{\text{X-PR-HSP-EPR-INFO}}$, where $X \in \{\text{CH}, \text{BTA}, \text{XR}\}$	
In:	$S_{\text{X-ACC-REQS-NHCP}}, S_{\text{X-ACC-REQS-HCP}}, S_{\text{X-PR-REQS}}, S_{\text{X-INFO-UNC-PO}} : M^*$
Out:	$K_{\text{X-PR-HSP-EPR-INFO}} : \mathbb{R}$
Description:	$K_{\text{X-PR-HSP-EPR-INFO}}$ = "The number of times since the monitoring started that health-care professionals or employees that are not health-care professionals have found printouts of highly sensitive and private information from EPRs on printers at X"

Requirements for $K_{\text{PR-HSP-EPR-INFO}}$	
In:	$S_{\text{CH-ACC-REQS-NHCP}}, S_{\text{BTA-ACC-REQS-NHCP}}, S_{\text{XR-ACC-REQS-NHCP}} : M^*$ $S_{\text{CH-ACC-REQS-HCP}}, S_{\text{BTA-ACC-REQS-HCP}}, S_{\text{XR-ACC-REQS-HCP}} : M^*$ $S_{\text{CH-PR-REQS}}, S_{\text{BTA-PR-REQS}}, S_{\text{XR-PR-REQS}} : M^*$ $S_{\text{CH-INFO-UNC-PO}}, S_{\text{BTA-INFO-UNC-PO}}, S_{\text{XR-INFO-UNC-PO}} : M^*$
Out:	$K_{\text{PR-HSP-EPR-INFO}} : \mathbb{R}$
Description:	$K_{\text{PR-HSP-EPR-INFO}} = \frac{10 \cdot (K_{\text{CH-PR-HSP-EPR-INFO}} + K_{\text{BTA-PR-HSP-EPR-INFO}} + K_{\text{XR-PR-HSP-EPR-INFO}})}{\textit{Number of years since the monitoring started}}$

lected printouts of information from EPRs by security employees at Client H, Blood test analysis, and X-ray, respectively.

B. Specify requirements to key indicators wrt deployed sensors (Step 3.2 of ValidKI)

Two key indicators $K_{\text{PR-SP-EPR-INFO}}$ and $K_{\text{PR-HSP-EPR-INFO}}$ are identified to monitor the likelihood values of the two unacceptable risks $R1\&R2$ and $R3\&R4$, respectively. In Tables V and VI their requirements are given. The two key indicators calculate likelihoods with respect to a ten year period, because the likelihoods in the likelihood scale in Table I are defined with respect to a ten year period. Both key indicators are composed of basic key indicators. Table V presents the requirements to the basic key indicators that $K_{\text{PR-SP-EPR-INFO}}$ is composed of, while Table VI presents the requirements to the basic key indicators that $K_{\text{PR-HSP-EPR-INFO}}$ is composed of.

For each key indicator we specify required sensor data. All of the key indicators rely on sequences of data

TABLE VII
KEY INDICATOR REQUIREMENTS SPECIFICATIONS FOR THE COMPOSITE KEY INDICATOR $K_{\text{NOT-APP-UNAUTH-ACC}}$ AND THE BASIC KEY INDICATORS $K_{\text{CH-NOT-APP-UNAUTH-ACC}}$, $K_{\text{BTA-NOT-APP-UNAUTH-ACC}}$, AND $K_{\text{XR-NOT-APP-UNAUTH-ACC}}$

Requirements for $K_{\text{X-NOT-APP-UNAUTH-ACC}}$, where $X \in \{\text{CH}, \text{BTA}, \text{XR}\}$	
In:	$S_{\text{X-AUTH-LIST}}, S_{\text{X-ACC-INFO-EPR}} : M^*$
Out:	$K_{\text{X-NOT-APP-UNAUTH-ACC}} : \mathbb{N}$
Description:	$K_{\text{X-NOT-APP-UNAUTH-ACC}}$ = "The number of not approved unauthorized accesses at X since the monitoring started to highly sensitive and private information in EPRs, where the owners of the EPRs are not patients of the accessors"

Requirements for $K_{\text{NOT-APP-UNAUTH-ACC}}$	
In:	$S_{\text{CH-AUTH-LIST}}, S_{\text{BTA-AUTH-LIST}}, S_{\text{XR-AUTH-LIST}} : M^*$ $S_{\text{CH-ACC-INFO-EPR}}, S_{\text{BTA-ACC-INFO-EPR}}, S_{\text{XR-ACC-INFO-EPR}} : M^*$
Out:	$K_{\text{NOT-APP-UNAUTH-ACC}} : \mathbb{R}$
Description:	$K_{\text{NOT-APP-UNAUTH-ACC}} = \frac{10 \cdot (K_{\text{CH-NOT-APP-UNAUTH-ACC}} + K_{\text{BTA-NOT-APP-UNAUTH-ACC}} + K_{\text{XR-NOT-APP-UNAUTH-ACC}})}{Number\ of\ years\ since\ the\ monitoring\ started}$

TABLE VIII
KEY INDICATOR REQUIREMENTS SPECIFICATIONS FOR THE COMPOSITE KEY INDICATOR $K_{\text{SP-EPR-INFO}}$ AND THE BASIC KEY INDICATORS $K_{\text{CH-SP-EPR-INFO}}$, $K_{\text{BTA-SP-EPR-INFO}}$, AND $K_{\text{XR-SP-EPR-INFO}}$

Requirements for $K_{\text{X-SP-EPR-INFO}}$, where $X \in \{\text{CH}, \text{BTA}, \text{XR}\}$	
In:	$S_{\text{X-ACC-INFO-EPR}}, S_{\text{X-INFO-GP}}, S_{\text{X-INFO-MRS}} : M^*$
Out:	$K_{\text{X-SP-EPR-INFO}} : \mathbb{N}$
Description:	$K_{\text{X-SP-EPR-INFO}}$ = "The number of times since the monitoring started that sensitive and private information from patients' EPRs have been shared by health-care professionals with others and where this information have ended up in the traditional media or on the Internet"

Requirements for $K_{\text{SP-EPR-INFO}}$	
In:	$S_{\text{CH-ACC-INFO-EPR}}, S_{\text{BTA-ACC-INFO-EPR}}, S_{\text{XR-ACC-INFO-EPR}} : M^*$ $S_{\text{CH-INFO-GP}}, S_{\text{BTA-INFO-GP}}, S_{\text{XR-INFO-GP}} : M^*$ $S_{\text{CH-INFO-MRS}}, S_{\text{BTA-INFO-MRS}}, S_{\text{XR-INFO-MRS}} : M^*$
Out:	$K_{\text{SP-EPR-INFO}} : \mathbb{R}$
Description:	$K_{\text{SP-EPR-INFO}} = \frac{10 \cdot (K_{\text{CH-SP-EPR-INFO}} + K_{\text{BTA-SP-EPR-INFO}} + K_{\text{XR-SP-EPR-INFO}})}{Number\ of\ years\ since\ the\ monitoring\ started}$

messages (M^*) gathered by the different sensors. We also specify the output type and requirements to output. For a key indicator K we refer to its requirement description as $Req(K)$.

Key indicators have also been identified for monitoring the unacceptable risks $R8$, $R10$, $R12$, and $R16\&R18$. Tables VII, VIII, IX, and X specify requirements to key indicators for monitoring the likelihood values of the risks $R8$, $R10$, $R12$, and $R16\&R18$, respectively.

TABLE IX
KEY INDICATOR REQUIREMENTS SPECIFICATIONS FOR THE COMPOSITE KEY INDICATOR $K_{\text{HSP-EPR-INFO}}$ AND THE BASIC KEY INDICATORS $K_{\text{CH-HSP-EPR-INFO}}$, $K_{\text{BTA-HSP-EPR-INFO}}$, AND $K_{\text{XR-HSP-EPR-INFO}}$

Requirements for $K_{\text{X-HSP-EPR-INFO}}$, where $X \in \{\text{CH}, \text{BTA}, \text{XR}\}$	
In:	$S_{\text{X-ACC-INFO-EPR}}, S_{\text{X-INFO-GP}}, S_{\text{X-INFO-MRS}} : M^*$
Out:	$K_{\text{X-HSP-EPR-INFO}} : \mathbb{N}$
Description:	$K_{\text{X-HSP-EPR-INFO}}$ = "The number of times since the monitoring started that highly sensitive and private information from patients' EPRs have been shared by health-care professionals with others and where this information have ended up in the traditional media or on the Internet"

Requirements for $K_{\text{HSP-EPR-INFO}}$	
In:	$S_{\text{CH-ACC-INFO-EPR}}, S_{\text{BTA-ACC-INFO-EPR}}, S_{\text{XR-ACC-INFO-EPR}} : M^*$ $S_{\text{CH-INFO-GP}}, S_{\text{BTA-INFO-GP}}, S_{\text{XR-INFO-GP}} : M^*$ $S_{\text{CH-INFO-MRS}}, S_{\text{BTA-INFO-MRS}}, S_{\text{XR-INFO-MRS}} : M^*$
Out:	$K_{\text{HSP-EPR-INFO}} : \mathbb{R}$
Description:	$K_{\text{HSP-EPR-INFO}} = \frac{10 \cdot (K_{\text{CH-HSP-EPR-INFO}} + K_{\text{BTA-HSP-EPR-INFO}} + K_{\text{XR-HSP-EPR-INFO}})}{\textit{Number of years since the monitoring started}}$

TABLE X
KEY INDICATOR REQUIREMENTS SPECIFICATIONS FOR THE COMPOSITE KEY INDICATOR $K_{\text{ILL-ACC-SC}}$ AND THE BASIC KEY INDICATORS $K_{\text{CH-ILL-ACC-SC}}$, $K_{\text{BTA-ILL-ACC-SC}}$, AND $K_{\text{XR-ILL-ACC-SC}}$

Requirements for $K_{\text{X-ILL-ACC-SC}}$, where $X \in \{\text{CH}, \text{BTA}, \text{XR}\}$	
In:	$S_{\text{X-REG-MIS-SC}}, S_{\text{X-ACC-INFO-EPR}} : M^*$
Out:	$K_{\text{X-ILL-ACC-SC}} : \mathbb{N}$
Description:	$K_{\text{X-ILL-ACC-SC}}$ = "The number of illegal accesses at X since the monitoring started to highly sensitive and private information in EPRs from lost/stolen smart cards"

Requirements for $K_{\text{ILL-ACC-SC}}$	
In:	$S_{\text{CH-REG-MIS-SC}}, S_{\text{BTA-REG-MIS-SC}}, S_{\text{XR-REG-MIS-SC}} : M^*$ $S_{\text{CH-ACC-INFO-EPR}}, S_{\text{BTA-ACC-INFO-EPR}}, S_{\text{XR-ACC-INFO-EPR}} : M^*$
Out:	$K_{\text{ILL-ACC-SC}} : \mathbb{R}$
Description:	$K_{\text{ILL-ACC-SC}} = \frac{10 \cdot (K_{\text{CH-ILL-ACC-SC}} + K_{\text{BTA-ILL-ACC-SC}} + K_{\text{XR-ILL-ACC-SC}})}{\textit{Number of years since the monitoring started}}$

VII. EVALUATE INTERNAL VALIDITY

A. Express business objective in terms of key indicators (Step 4.1 of ValidKI)

The precise business objective PBO-A8' is a reformulation of the precise business objective PBO-A8 expressed in terms of key indicators.

$$\begin{aligned}\text{PBO-A8'} = {} & K_{\text{PR-SP-EPR-INFO}} \in [0, 19] \ \wedge \ Req(K_{\text{SP-PR-EPR-INFO}}) \ \wedge \\ & K_{\text{PR-HSP-EPR-INFO}} \in [0, 5] \ \wedge \ Req(K_{\text{HSP-PR-EPR-INFO}}) \ \wedge \\ & K_{\text{NOT-APP-UNAUTH-ACC}} \in [0, 5] \ \wedge \ Req(K_{\text{NOT-APP-UNAUTH-ACC}}) \ \wedge \\ & K_{\text{SP-EPR-INFO}} \in [0, 5] \ \wedge \ Req(K_{\text{SP-EPR-INFO}}) \ \wedge \\ & K_{\text{HSP-EPR-INFO}} \in [0, 1] \ \wedge \ Req(K_{\text{HSP-EPR-INFO}}) \ \wedge \\ & K_{\text{ILL-ACC-SC}} \in [0, 1] \ \wedge \ Req(K_{\text{ILL-ACC-SC}})\end{aligned}$$

The precise business objective PBO-A8 is fulfilled if the likelihood values of the six unacceptable risks $R1\&R2$, $R3\&R4$, $R8$, $R10$, $R12$, and $R16\&R18$ change in such a way that the six risks become acceptable. The risks become acceptable if their likelihood values change in the following way:

TABLE XI
THE RISK EVALUATION MATRIX WHEN THE PRECISE BUSINESS OBJECTIVE PBO-A8 IS FULFILLED

Likelihood \ **Consequence**	Insignificant	Minor	Moderate	Major	Catastrophic
Rare			$R1\&R2'$	$R3\&R4'$, $R8'$, $R10'$, $R15\&R17$	$R12$, $R16\&R18$
Unlikely			$R1\&R2''$	$R3\&R4''$, $R8''$, $R10''$	
Possible		$R6$, $R7$	$R1\&R2'''$, $R9$, $R11$		
Likely	$R13$	$R5$, $R14$			
Certain					

- The risk $R1\&R2$ becomes acceptable if the likelihood changes from "Likely" to "Possible," "Unlikely," or "Rare." The likelihood will change in such a way if the composite key indicator $K_{\text{PR-SP-EPR-INFO}}$, monitoring the likelihood, is contained in the interval $[0, 19]$ (interval capturing both "Rare: $[0, 1]$: 10 years," "Unlikely: $[2, 5]$: 10 years," and "Possible: $[6, 19]$: 10 years").
- The risk $R3\&R4$ becomes acceptable if the likelihood changes from "Possible" to "Unlikely" or "Rare." The likelihood will change in such a way if the composite key indicator $K_{\text{PR-HSP-EPR-INFO}}$, monitoring the likelihood, is contained in the interval $[0, 5]$ (interval capturing both "Rare: $[0, 1]$: 10 years" and "Unlikely: $[2, 5]$: 10 years").
- The risk $R8$ becomes acceptable if the likelihood changes from "Possible" to "Unlikely" or "Rare." The likelihood will change in such a way if the composite key indicator $K_{\text{NOT-APP-UNAUTH-ACC}}$, monitoring the likelihood, is contained in the interval $[0, 5]$ (interval capturing both "Rare: $[0, 1]$: 10 years" and "Unlikely: $[2, 5]$: 10 years").
- The risk $R10$ becomes acceptable if the likelihood changes from "Possible" to "Unlikely" or "Rare." The likelihood will change in such a way if the composite key indicator $K_{\text{SP-EPR-INFO}}$, monitoring the likelihood, is contained in the interval $[0, 5]$ (interval capturing both "Rare: $[0, 1]$: 10 years" and "Unlikely: $[2, 5]$: 10 years").
- The risk $R12$ becomes acceptable if the likelihood changes from "Unlikely" to "Rare." The likelihood will change in such a way if the composite key indicator $K_{\text{HSP-EPR-INFO}}$, monitoring the likelihood, is contained in the interval $[0, 1]$ (interval capturing "Rare: $[0, 1]$: 10 years").
- The risk $R16\&R18$ becomes acceptable if the likelihood changes from "Unlikely" to "Rare." The likelihood will change in such a way if the composite key indicator $K_{\text{ILL-ACC-SC}}$, monitoring the likelihood, is contained in the interval $[0, 1]$ (interval capturing "Rare: $[0, 1]$: 10 years").

Moreover, the different composite key indicators need to measure the likelihoods correctly in order to measure the fulfillment of PBO-A8. This can be determined based on the requirements to the different composite key indicators. These requirements are captured by $Req(K_{\text{PR-SP-EPR-INFO}})$, $Req(K_{\text{PR-HSP-EPR-INFO}})$, etc.

The reformulated precise business objective can also be used to determine to what degree the precise business objective is fulfilled. For instance, if $K_{\text{PR-SP-EPR-INFO}}$ equals 20 while the other composite key indicators equal 0, then PBO-A8 is close to being fulfilled. On the other hand, if $K_{\text{PR-SP-EPR-INFO}}$ equals 25 instead, then PBO-A8 is far from being fulfilled.

B. Evaluate criteria for internal validity (Step 4.2 of ValidKI)

To evaluate the internal validity of the set of key indicators, we need to show that the reformulated precise business objective PBO-A8' measures the fulfillment of the precise business objective PBO-A8. We evaluate the internal validity of each composite key indicator based on the criteria given in Section III-D.

To evaluate attribute validity we need to compare the definitions of the six risks with the requirements to the composite key indicators. The definitions of the risks $R8$, $R10$, and $R12$ are given in Figs. 7 and 8, while the definitions of the accumulated risks $R1\&R2$, $R3\&R4$, and $R16\&R18$ are given in Section V-C. Moreover, the

requirements to the composite key indicators are given by $Req(K_{\text{PR-SP-EPR-INFO}})$, $Req(K_{\text{PR-HSP-EPR-INFO}})$, etc. In all six cases there is a match between the definition of the risk and the requirements to the composite key indicator. We therefore conclude that the composite key indicators correctly exhibit the likelihood attributes of the six risks that the composite key indicators intend to measure. In addition, based on the requirements specified for the six composite key indicators it is clear that the six composite key indicators are not restricted to only producing values that are always contained or not contained in the intervals mentioned above. Thus, both acceptable and unacceptable risks can be detected.

Moreover, all the composite key indicators have factor independence. Each composite key indicator is calculated based on three basic key indicators. These are independent of each other, since they are computed by three different health-care institutions. The six composite key indicators do also have internal consistency, since the three basic key indicators employed by each composite key indicator measure the same thing, but at different health-care institutions. The three basic key indicators are therefore conceptually related.

We continue the evaluation of internal validity by evaluating whether the composite key indicators have appropriate continuity. All are discontinuous if *"Number of years since the monitoring started"* equals zero. Client H does not consider this to be a problem, since the denominator will in all six cases be a real number that is never zero. We also show that the six composite key indicators have dimensional consistency. Each composite key indicator adds three likelihoods, where each is for the period of *"Number of years since the monitoring started"* years, and transforms the resulting likelihood into a likelihood which is for a period of ten years. Thus, no information is lost when constructing the composite key indicators from their respective basic key indicators. The six composite key indicators do also have unit validity. All six use the unit "likelihood per ten years," which is appropriate for measuring the six likelihood attributes of the risks.

Based on the evaluation of the different internal validity types of criteria above, we conclude that the set of key indicators is internally valid. When the precise business objective PBO-A8 is fulfilled, we get the risk evaluation matrix in Table XI. In this situation, all of the risks $R1\&R2$, $R3\&R4$, $R8$, $R10$, $R12$, and $R16\&R18$ are acceptable. Moreover, the risks will have the following likelihood values when acceptable:

- The risk $R1\&R2$ will either have the likelihood "Rare" ($R1\&R2'$), "Unlikely" ($R1\&R2''$), or "Possible" ($R1\&R2'''$).
- The risk $R3\&R4$ will either have the likelihood "Rare" ($R3\&R4'$) or "Unlikely" ($R3\&R4''$).
- The risk $R8$ will either have the likelihood "Rare" ($R8'$) or "Unlikely" ($R8''$).
- The risk $R10$ will either have the likelihood "Rare" ($R10'$) or "Unlikely" ($R10''$).
- The risk $R12$ will have the likelihood "Rare".
- The risk $R16\&R18$ will have the likelihood "Rare".

VIII. Specify key indicator designs

We use the UML [6] sequence diagram notation for the key indicator design specifications, but one may of course also use other languages depending on the problem in question. In the following sub-sections, we specify the designs of the six composite key indicators and their respective basic key indicators.

A. Key indicator designs for $K_{\text{PR-SP-EPR-INFO}}$ and its basic key indicators

The sequence diagram in Fig. 11 specifies how the key indicator $K_{\text{PR-SP-EPR-INFO}}$ is calculated. Each entity in the sequence diagram is either a component, a sensor, or an employee at Client H, and it is represented by a dashed, vertical line called a lifeline, where the box at its top specifies which entity the lifeline represents. The entities interact with each other through the transmission and reception of messages, which are shown as horizontal arrows from the transmitting lifeline to the receiving lifeline. We can also see that a lifeline can be both the sender and receiver of a message.

The sequence diagram contains one reference (ref) to another sequence diagram. This reference can be replaced by the content of the sequence diagram that it refers to. The reference refers to the sequence diagram given in Fig. 12, which describes the calculation of the basic key indicator $K_{\text{CH-PR-SP-EPR-INFO}}$ at Client H. We do not present sequence diagrams describing the calculations of the two other basic key indicators, since these calculations are performed in the same way as the calculation of $K_{\text{CH-PR-SP-EPR-INFO}}$, and since these calculations involve the same

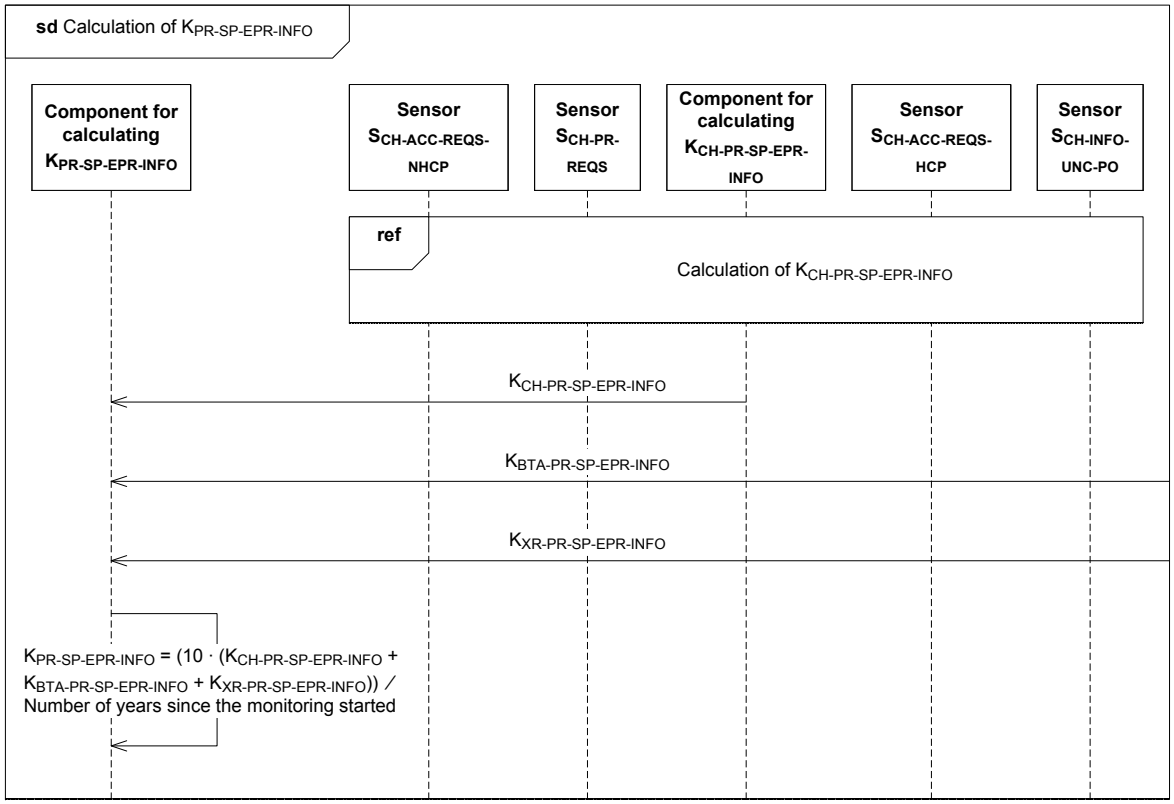

Fig. 11. The sequence diagram "Calculation of $K_{\text{PR-SP-EPR-INFO}}$"

types of lifelines as the ones described in Fig. 12. For the two other basic key indicators we only show that they are sent to "Component for calculating $K_{\text{PR-SP-EPR-INFO}}$," and that they are used in the calculation of $K_{\text{PR-SP-EPR-INFO}}$.

The sequence diagram in Fig. 12 shows that the basic key indicator $K_{\text{CH-PR-SP-EPR-INFO}}$ is updated each week. The first thing that happens is that "Component for calculating $K_{\text{CH-PR-SP-EPR-INFO}}$" retrieves the value that was computed for the basic key indicator in the previous week. Afterwards, the component counts for each printout the number of health-care professionals and employees that are not health-care professionals that accessed the printer room between TIME_1 (the time the print job was completed) and TIME_2 (the time when the health-care professional collected his/hers printout or the time when the printout was collected by a security employee). The number NUM is the number of other health-care professionals and employees that are not health-care professionals that may have seen the printout of sensitive and private information.

Client H is of the opinion that between 10% and 30% of the other health-care professionals and employees that are not health-care professionals that accessed the printer rooms between TIME_1 and TIME_2 have seen the printouts of sensitive and private information from patients' EPRs. Thus, the number TOTAL_NUM is multiplied by $[0.1, 0.3]$. In the end, the component stores the basic key indicator before sending it to "Component for calculating $K_{\text{PR-SP-EPR-INFO}}$," as illustrated in the sequence diagram in Fig. 11.

B. Key indicator designs for $K_{\text{PR-HSP-EPR-INFO}}$ and its basic key indicators

The sequence diagram in Fig. 13 specifies how the key indicator $K_{\text{PR-HSP-EPR-INFO}}$ is calculated, while the sequence diagram in Fig. 14 describes the calculation of the basic key indicator $K_{\text{CH-PR-HSP-EPR-INFO}}$ at Client H. We use the same argument as the one given in Section VIII-A for not presenting sequence diagrams for the two other basic key indicators.

The sequence diagram in Fig. 14 shows that the basic key indicator $K_{\text{CH-PR-HSP-EPR-INFO}}$ is updated each week. This sequence diagram is almost identical to the one in Fig. 12. Thus, we do not give any further explanations for the sequence diagram.

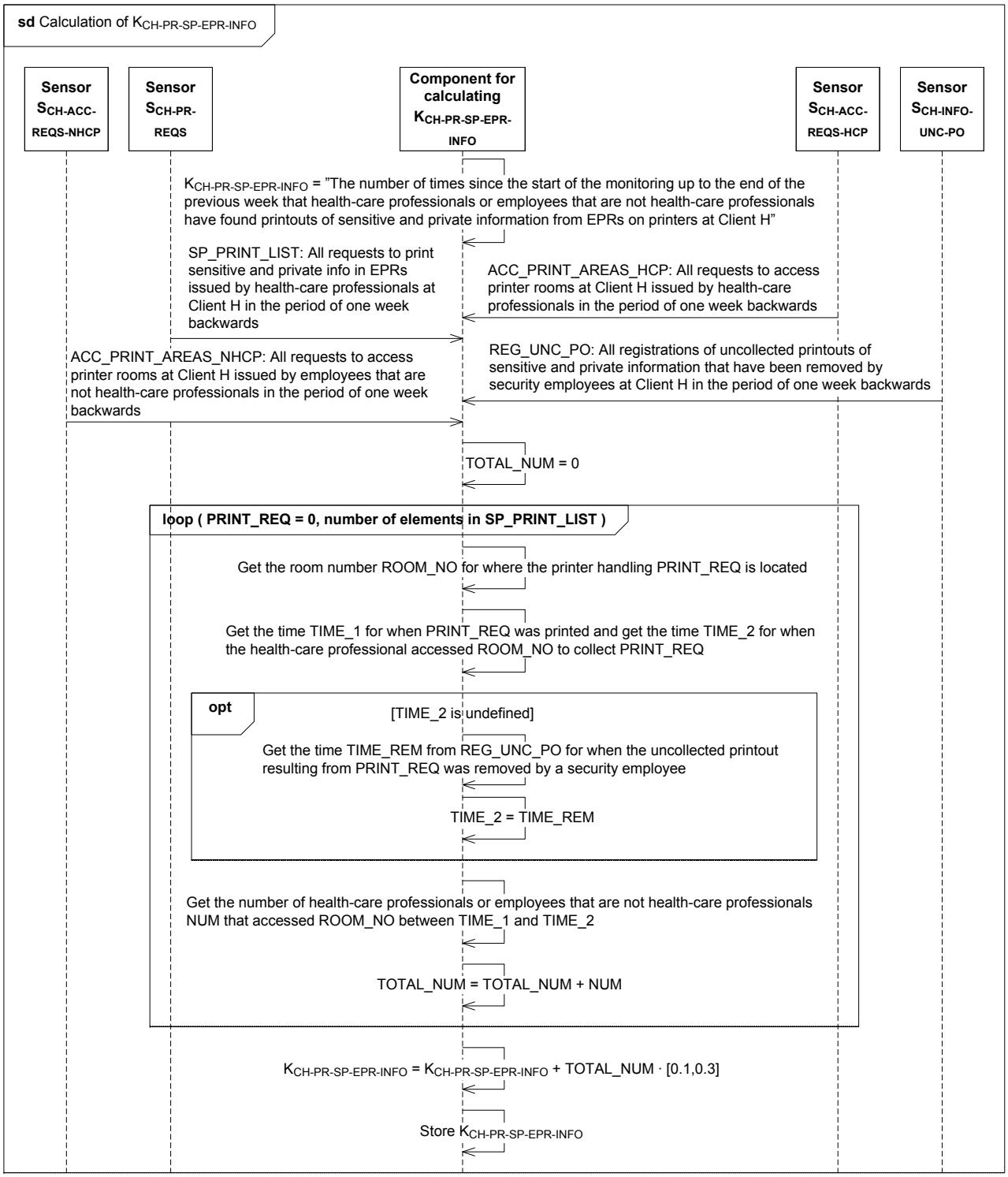

Fig. 12. The sequence diagram "Calculation of $K_{\text{CH-PR-SP-EPR-INFO}}$"

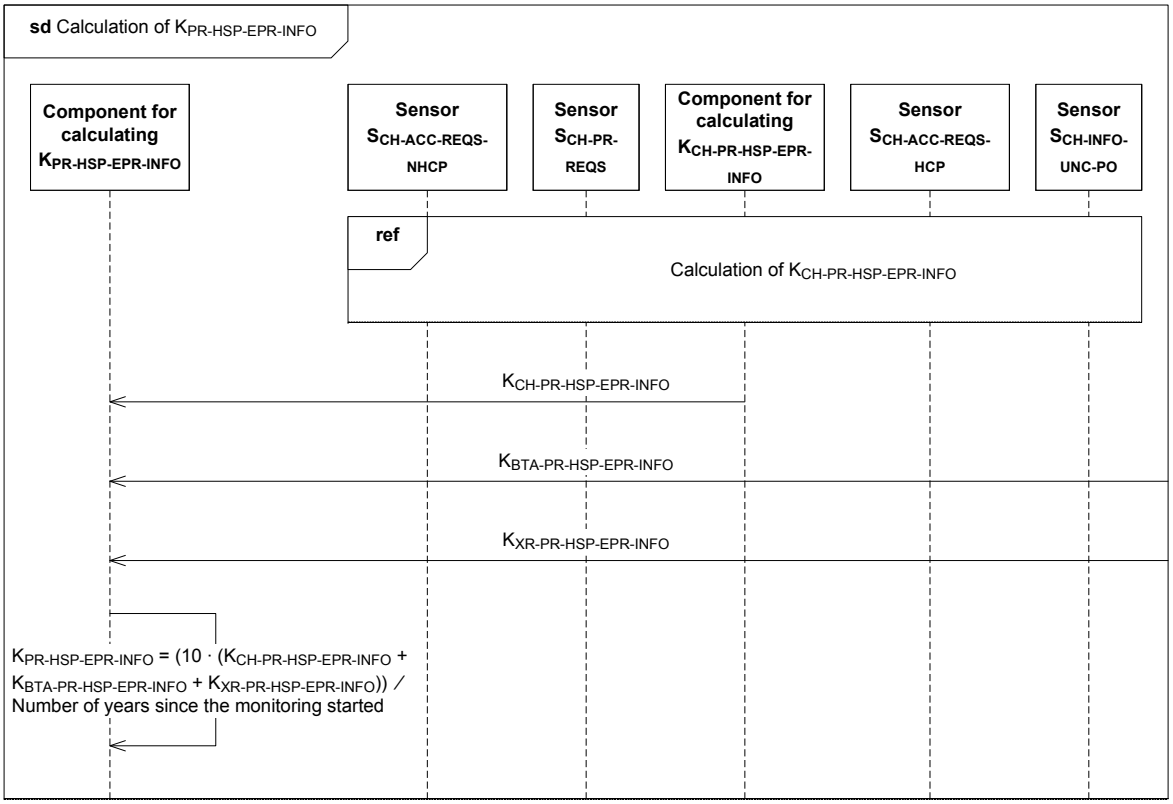

Fig. 13. The sequence diagram "Calculation of $K_{\text{PR-HSP-EPR-INFO}}$"

C. Key indicator designs for $K_{NOT\text{-}APP\text{-}UNAUTH\text{-}ACC}$ and its basic key indicators

The sequence diagram in Fig. 15 specifies how the key indicator $K_{\text{NOT-APP-UNAUTH-ACC}}$ is calculated, while the sequence diagram in Fig. 16 describes the calculation of the basic key indicator $K_{\text{CH-NOT-APP-UNAUTH-ACC}}$ at Client H. We use the same argument as the one given in Section VIII-A for not presenting sequence diagrams for the two other basic key indicators.

The sequence diagram in Fig. 16 shows that the basic key indicator $K_{\text{CH-NOT-APP-UNAUTH-ACC}}$ is updated each week. The first thing that happens is that "Component for calculating $K_{\text{CH-NOT-APP-UNAUTH-ACC}}$" sends the value that was computed for the basic key indicator in the previous week to "Employee at Client H." Afterwards, the component identifies "All unauthorized accesses at Client H in the period of one week backwards to highly sensitive and private information in EPRs, where the owners of the EPRs are not patients of the accessors" based on input from the entities representing the sensors. The "Employee at Client H" performs a manual inspection of each of these unauthorized accesses, and classifies each as approved or not approved. If the unauthorized access is classified as not approved, then the basic key indicator is incremented by one. After all the unauthorized accesses have been inspected and classified, "Employee at Client H" sends the basic key indicator to the component which stores it. Afterwards, the component sends the basic key indicator to "Component for calculating $K_{\text{NOT-APP-UNAUTH-ACC}}$," as illustrated in the sequence diagram in Fig. 15.

D. Key indicator designs for $K_{SP\text{-}EPR\text{-}INFO}$ and its basic key indicators

The sequence diagram in Fig. 17 specifies how the key indicator $K_{\text{SP-EPR-INFO}}$ is calculated, while the sequence diagram in Fig. 18 describes the calculation of the basic key indicator $K_{\text{CH-SP-EPR-INFO}}$ at Client H. We use the same argument as the one given in Section VIII-A for not presenting sequence diagrams for the two other basic key indicators.

The sequence diagram in Fig. 18 shows that the basic key indicator $K_{\text{CH-SP-EPR-INFO}}$ is updated each week. The first thing that happens is that "Component for calculating $K_{\text{CH-SP-EPR-INFO}}$" sends the value that was computed for the basic key indicator in the previous week to "Employee at Client H". Afterwards, the component receives

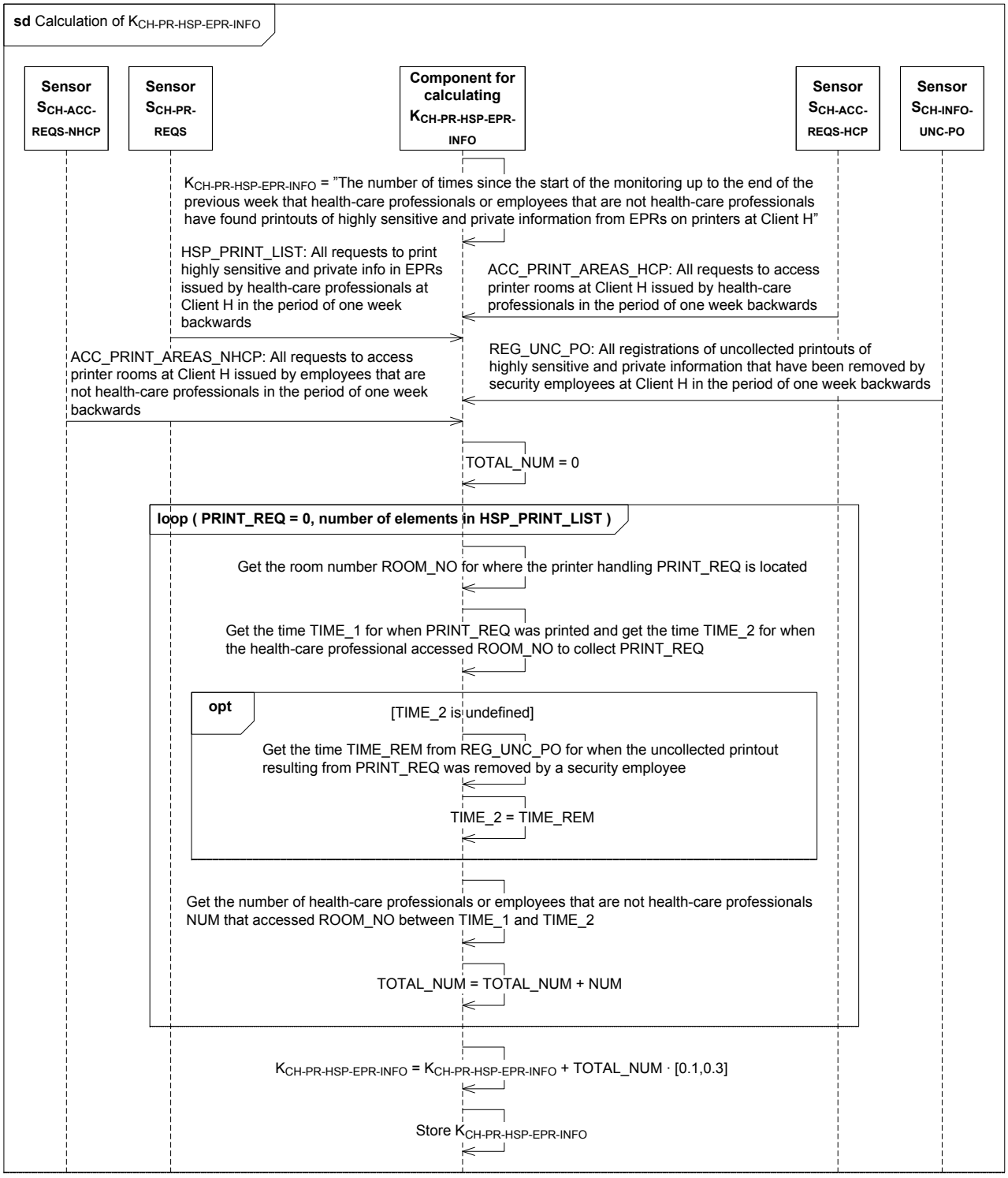

Fig. 14. The sequence diagram "Calculation of $K_{\text{CH-PR-HSP-EPR-INFO}}$"

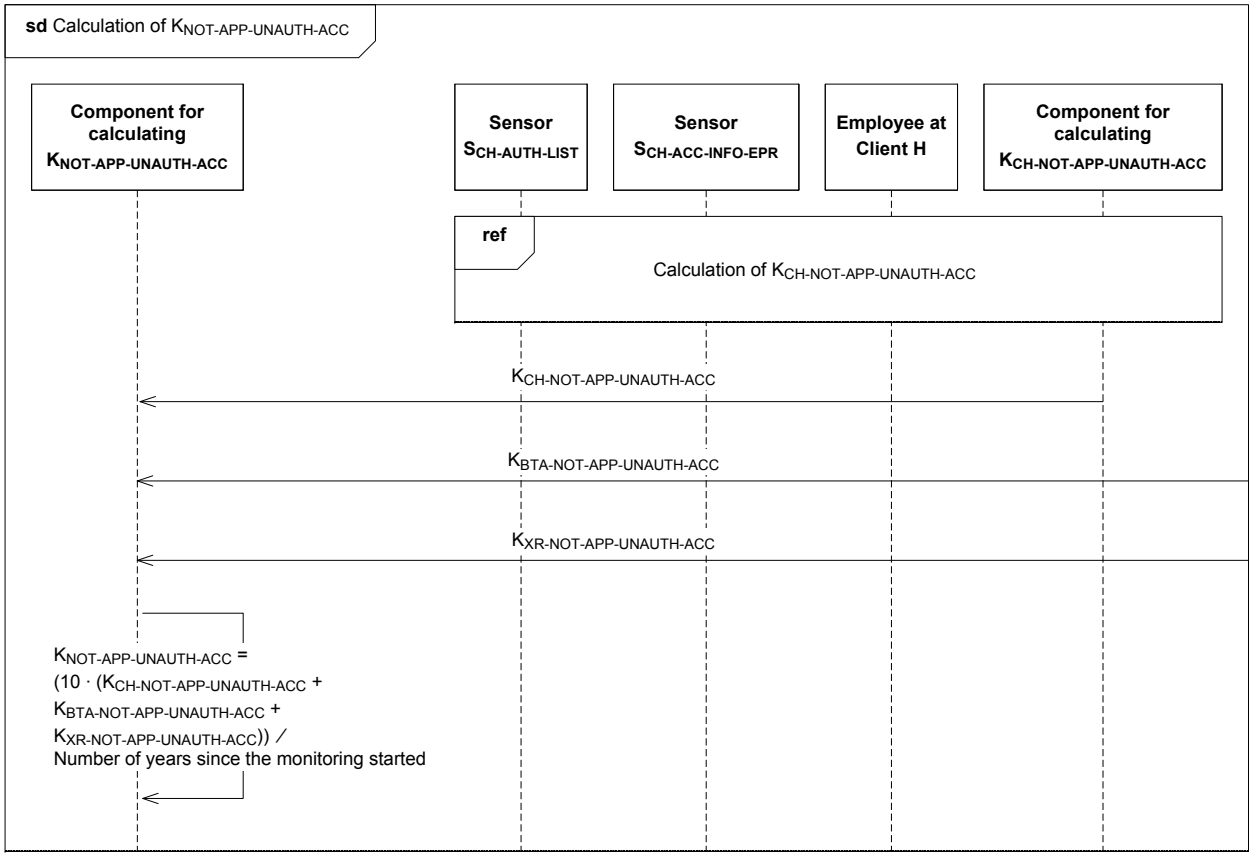

Fig. 15. The sequence diagram "Calculation of $K_{\text{NOT-APP-UNAUTH-ACC}}$"

different kinds of data from the three sensors, where this data is used in the sequence diagram "Comparison of data" in Fig. 19 for updating $K_{\text{CH-SP-EPR-INFO}}$.

In the sequence diagram in Fig. 19, "Component for calculating $K_{\text{CH-SP-EPR-INFO}}$" extracts all accesses to sensitive and private information in EPRs that have occurred in the period of one week backwards. The component also extracts all information items from INFO_LIST_1 and INFO_LIST_2 that both refer to Client H and the medical history of a person. Since information retrieved from the traditional media or the Internet will refer to patients by name, the different accesses are grouped with respect to patient names. In addition, duplicate accesses are removed, since we are not interested in how many times some information has been accessed, but rather whether it has been accessed or not. As can be seen in the sequence diagram, the different items of information retrieved from the traditional media or the Internet are grouped in the same way as for accesses to information in EPRs.

After having grouped the different data, we check for the different information items whether they match information that is retrieved when performing different accesses to information in EPRs. We use software to identify potential matches, while an employee at Client H performs a manual check of the potential matches to determine whether the sensitive and private information obtained from performing an access to information in an EPR is really the source of the information that has been retrieved from the traditional media or the Internet. When evaluating the potential matches, the employee needs to consider other potential sources for the information leakage, such as the patient itself. The employee also needs to consider whether the information retrieved from the traditional media or the Internet really refers to the same patient as the information obtained from an EPR does. If the employee is confident that the information from the EPR is the source, then the basic key indicator $K_{\text{CH-SP-EPR-INFO}}$ is incremented by one. In the end, the employee sends the updated basic key indicator to "Component for calculating $K_{\text{CH-SP-EPR-INFO}}$," as illustrated in Fig. 18. The component stores the updated basic key indicator before sending it to "Component for calculating $K_{\text{SP-EPR-INFO}}$," as illustrated in the sequence diagram in Fig. 17.

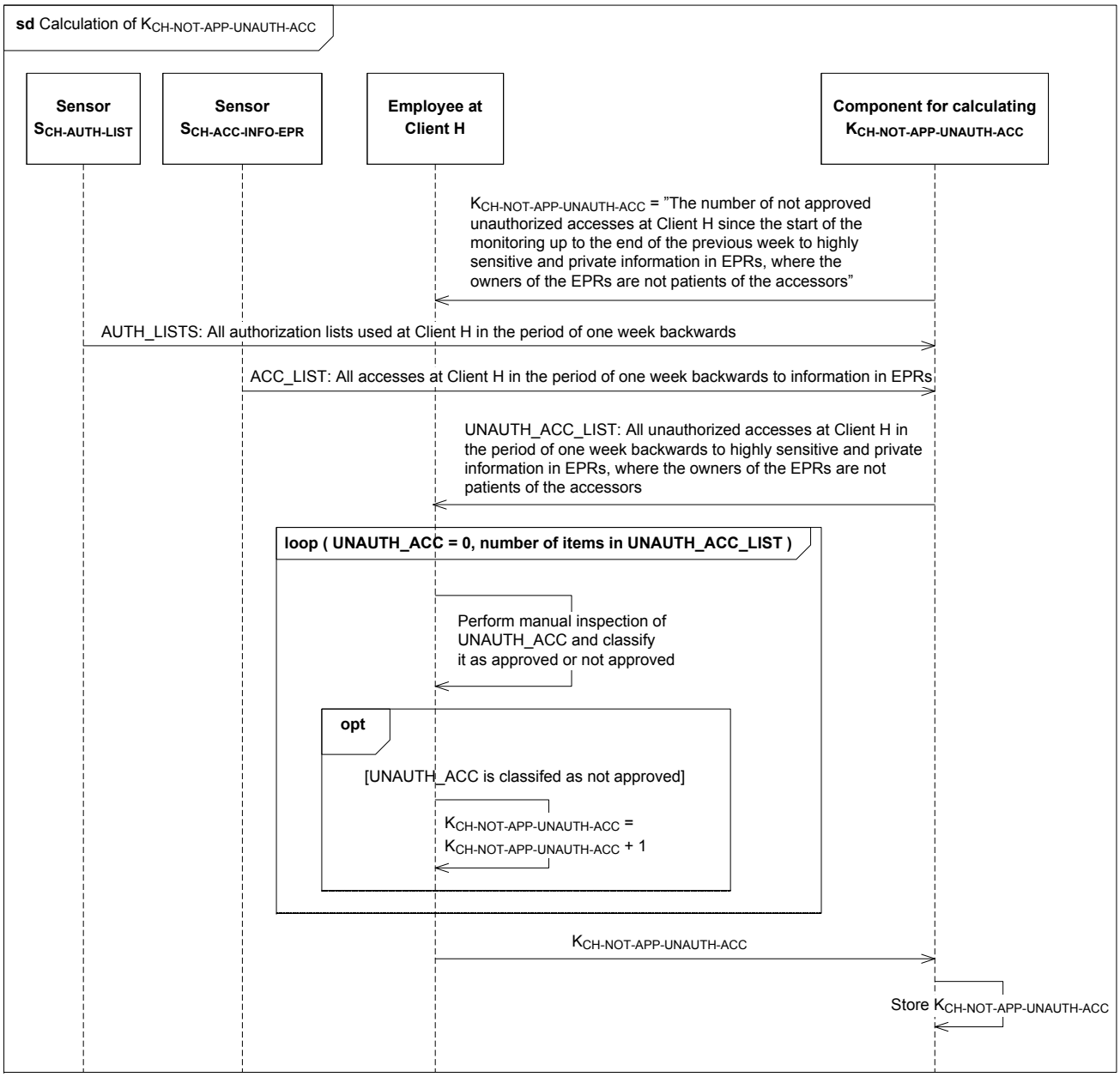

Fig. 16. The sequence diagram "Calculation of $K_{\text{CH-NOT-APP-UNAUTH-ACC}}$"

E. Key indicator designs for $K_{HSP\text{-}EPR\text{-}INFO}$ and its basic key indicators

The sequence diagram in Fig. 20 specifies how the key indicator $K_{\text{HSP-EPR-INFO}}$ is calculated, while the sequence diagram in Fig. 21 describes the calculation of the basic key indicator $K_{\text{CH-HSP-EPR-INFO}}$ at Client H. We use the same argument as the one given in Section VIII-A for not presenting sequence diagrams for the two other basic key indicators.

The sequence diagram in Fig. 21 shows that the basic key indicator $K_{\text{CH-HSP-EPR-INFO}}$ is updated each week. This sequence diagram is almost identical to the one in Fig. 18, while the sequence diagram "Comparison of data" in Fig. 22, which is referred to in Fig. 21, is almost identical to the one in Fig. 19. Thus, we do not give any further explanations for the two sequence diagrams.

F. Key indicator designs for $K_{ILL\text{-}ACC\text{-}SC}$ and its basic key indicators

The sequence diagram in Fig. 23 specifies how the key indicator $K_{\text{ILL-ACC-SC}}$ is calculated, while the sequence diagram in Fig. 24 describes the calculation of the basic key indicator $K_{\text{CH-ILL-ACC-SC}}$ at Client H. We use the same

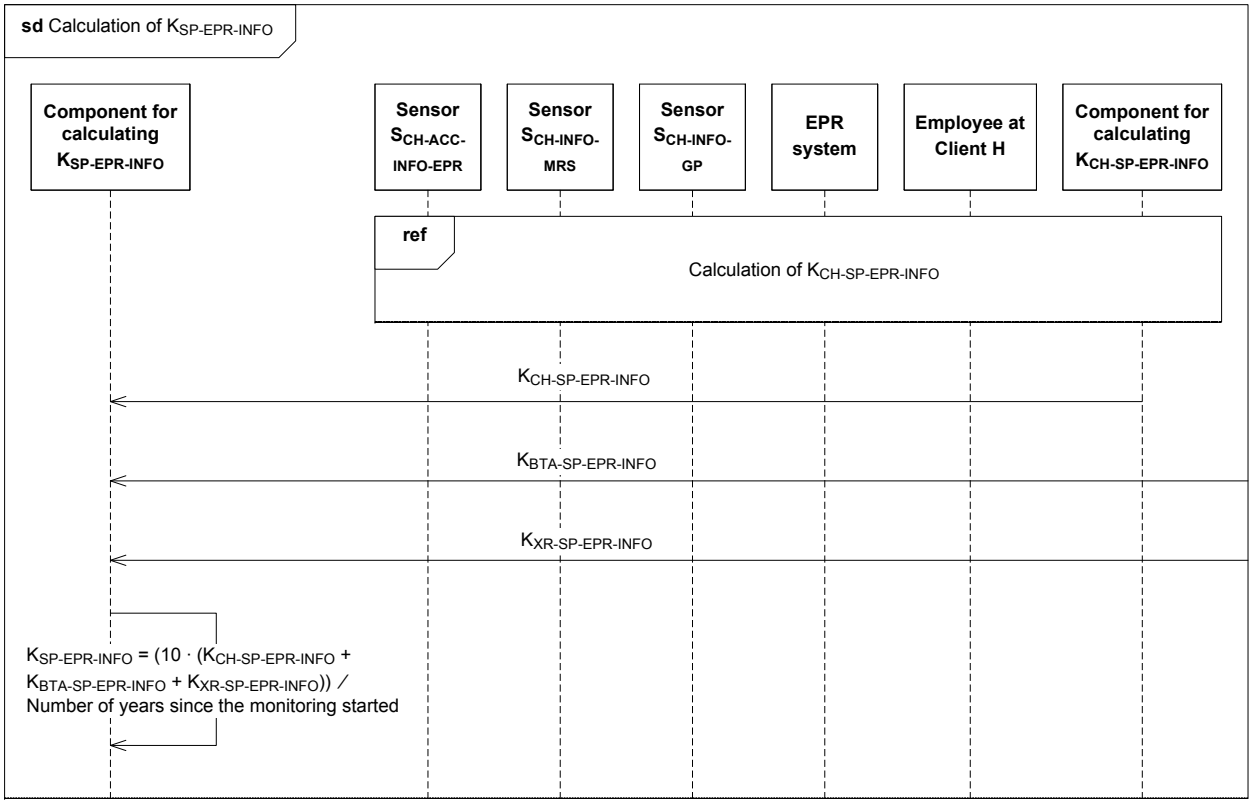

Fig. 17. The sequence diagram "Calculation of $K_{\text{SP-EPR-INFO}}$"

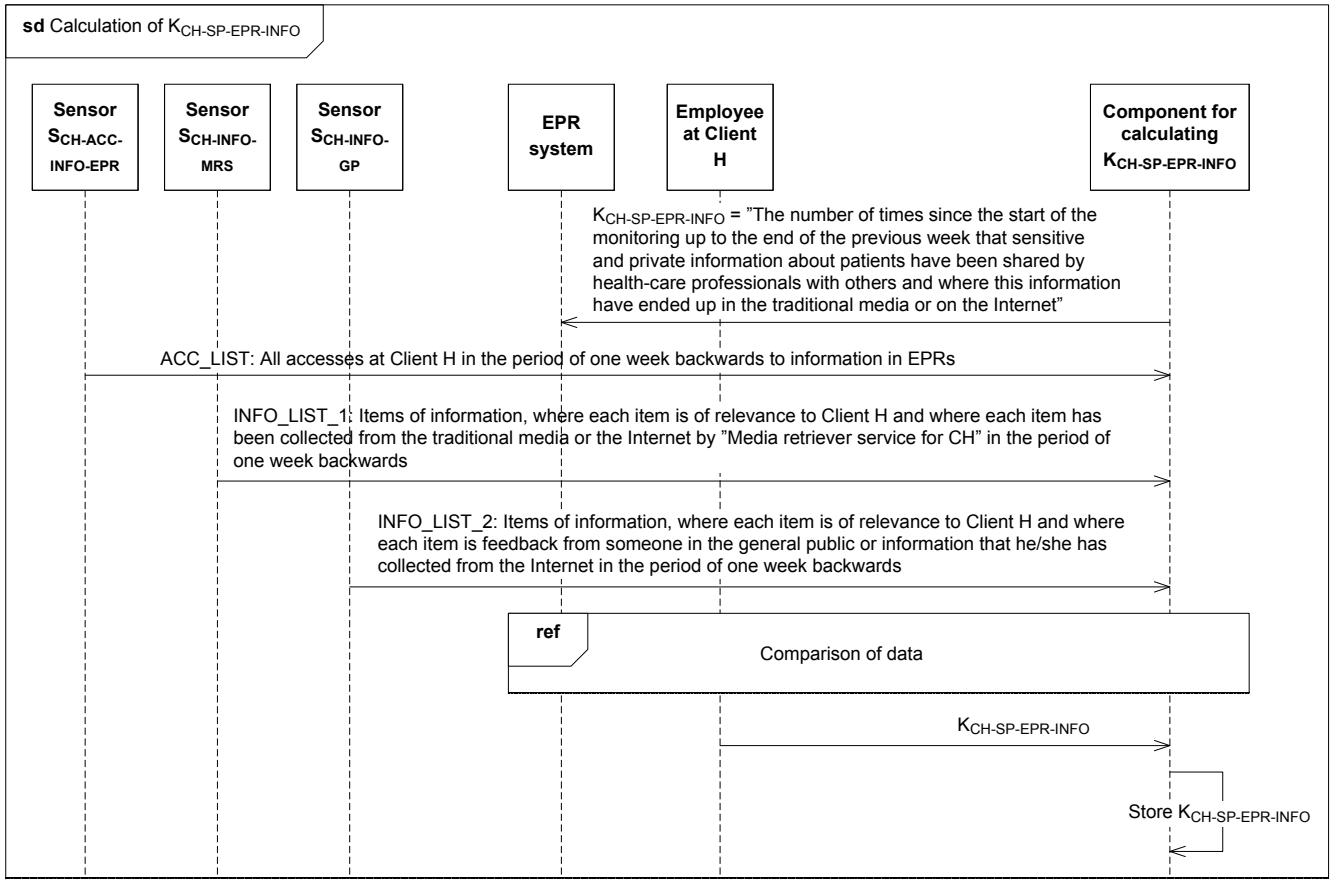

Fig. 18. The sequence diagram "Calculation of $K_{\text{CH-SP-EPR-INFO}}$"

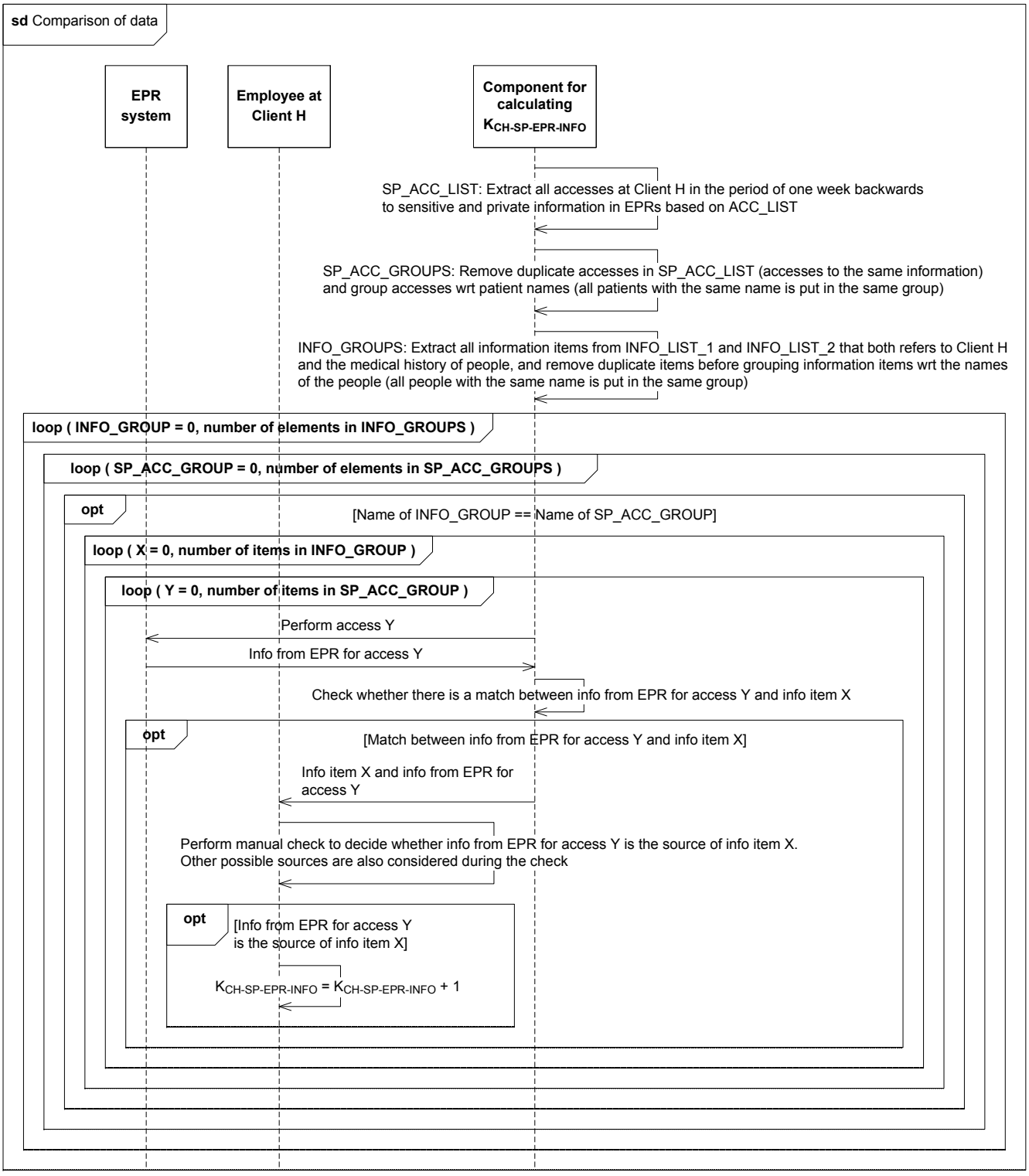

Fig. 19. The sequence diagram “Comparison of data”

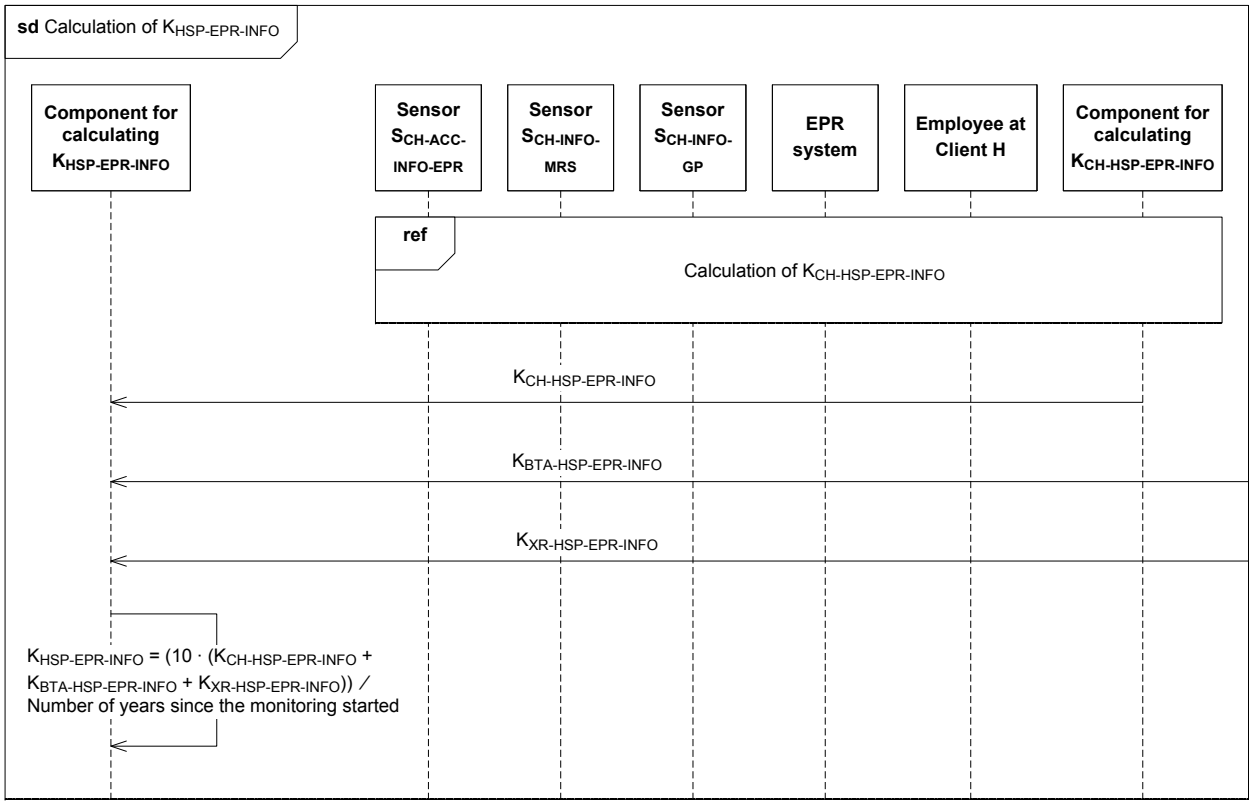

Fig. 20. The sequence diagram "Calculation of $K_{\text{HSP-EPR-INFO}}$"

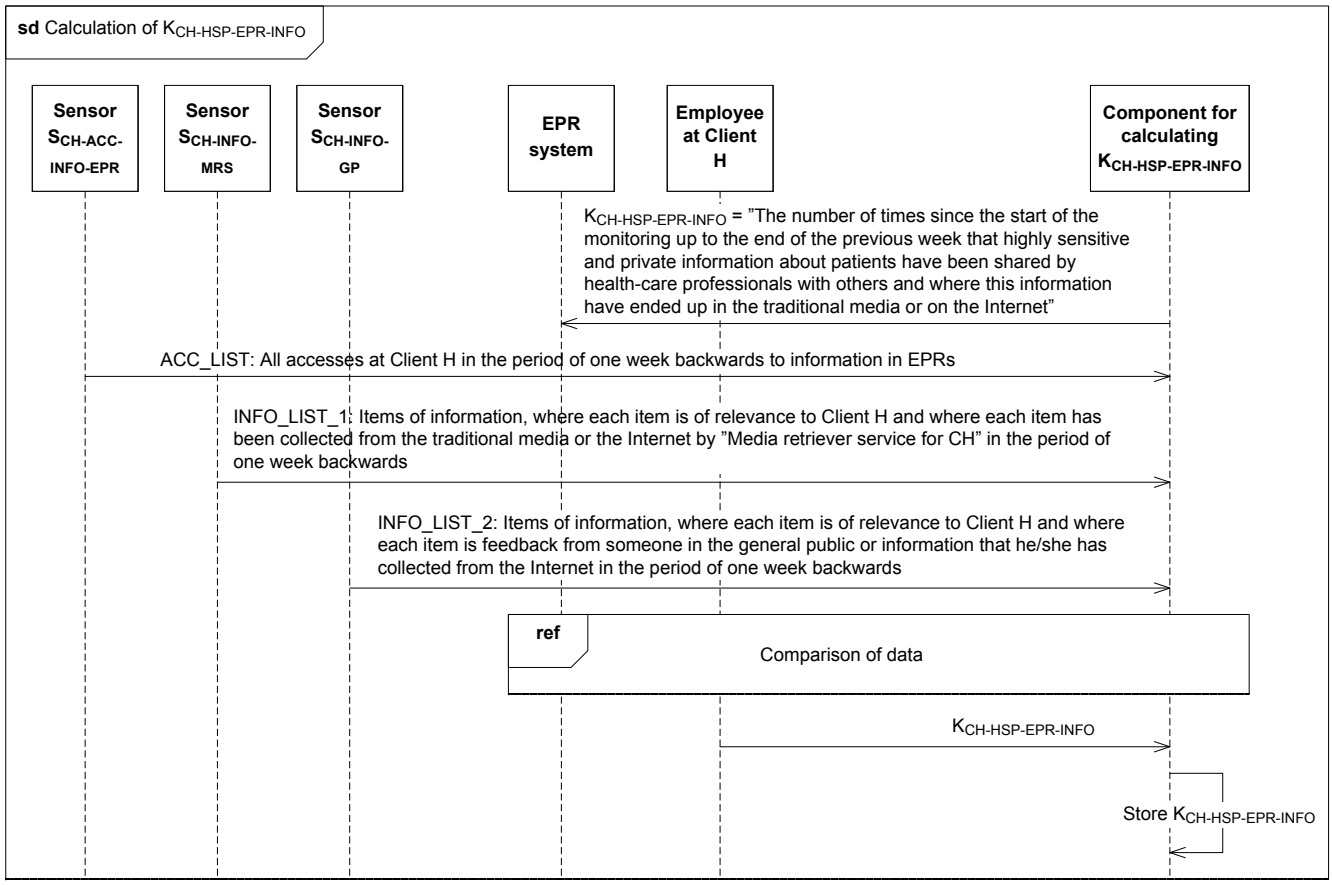

Fig. 21. The sequence diagram "Calculation of $K_{\text{CH-HSP-EPR-INFO}}$"

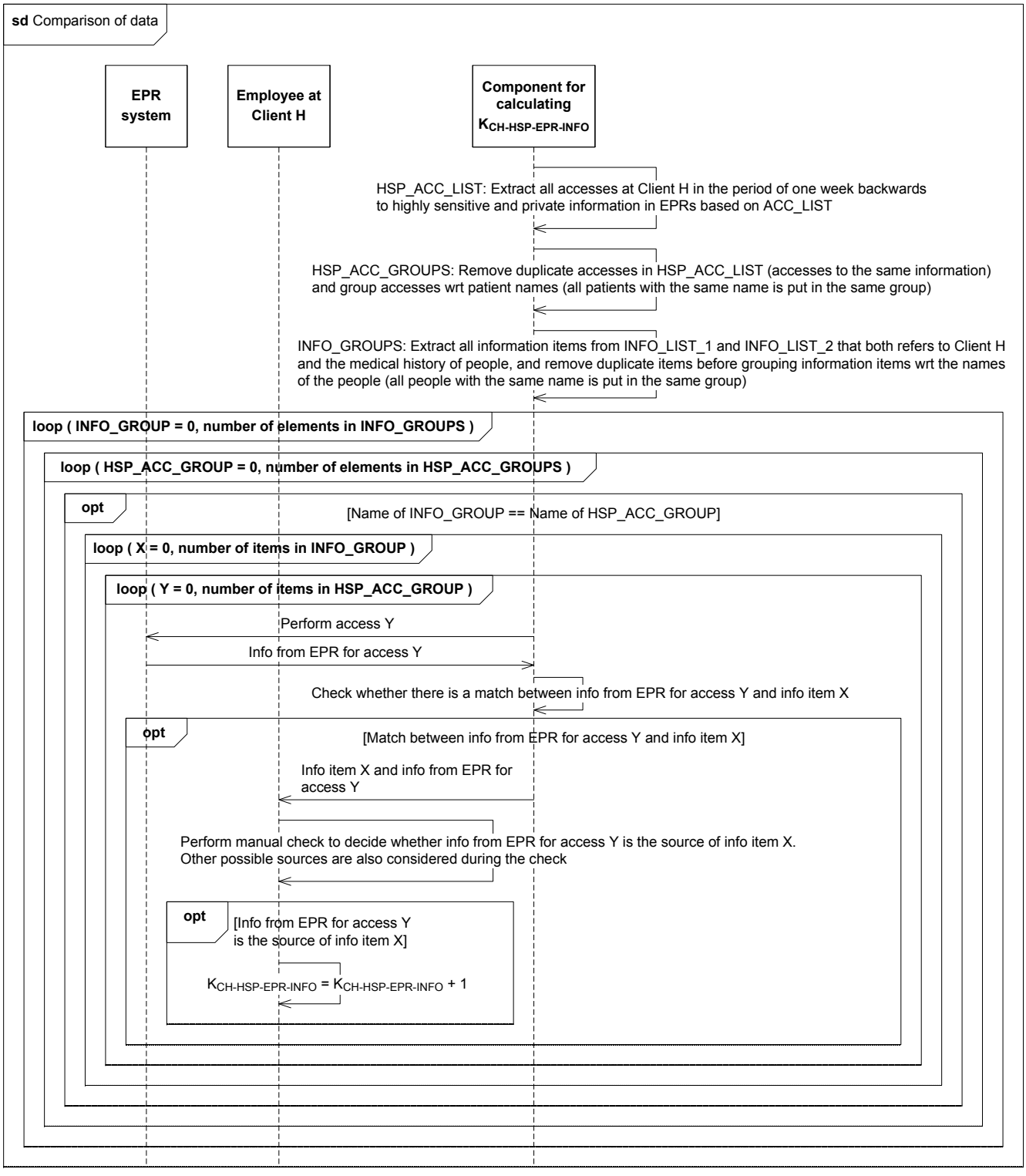

Fig. 22. The sequence diagram “Comparison of data”

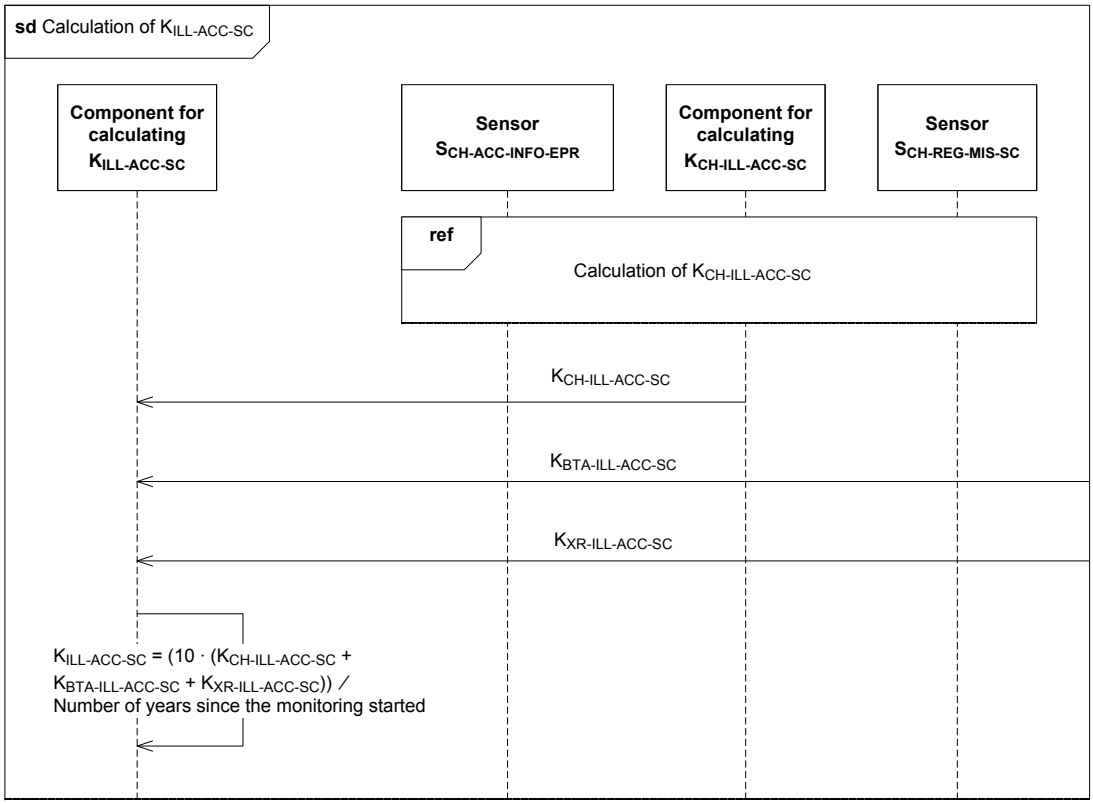

Fig. 23. The sequence diagram "Calculation of $K_{\text{ILL-ACC-SC}}$"

argument as the one given in Section VIII-A for not presenting sequence diagrams for the two other basic key indicators.

The sequence diagram in Fig. 24 shows that the basic key indicator $K_{\text{CH-ILL-ACC-SC}}$ is updated each week. The first thing that happens is that "Component for calculating $K_{\text{CH-ILL-ACC}}$" retrieves the value that was computed for the basic key indicator in the previous week. Afterwards, the component counts for each of the lost/stolen smart cards the number of accesses that have occurred between TIME_1 (the time the smart card's owner used it the last time before noticing that it was missing) and TIME_2 (the time when the smart card was registered as missing). In the end, the component stores the basic key indicator $K_{\text{CH-ILL-ACC-SC}}$, and sends it to "Component for calculating $K_{\text{ILL-ACC-SC}}$," as illustrated in the sequence diagram in Fig. 23.

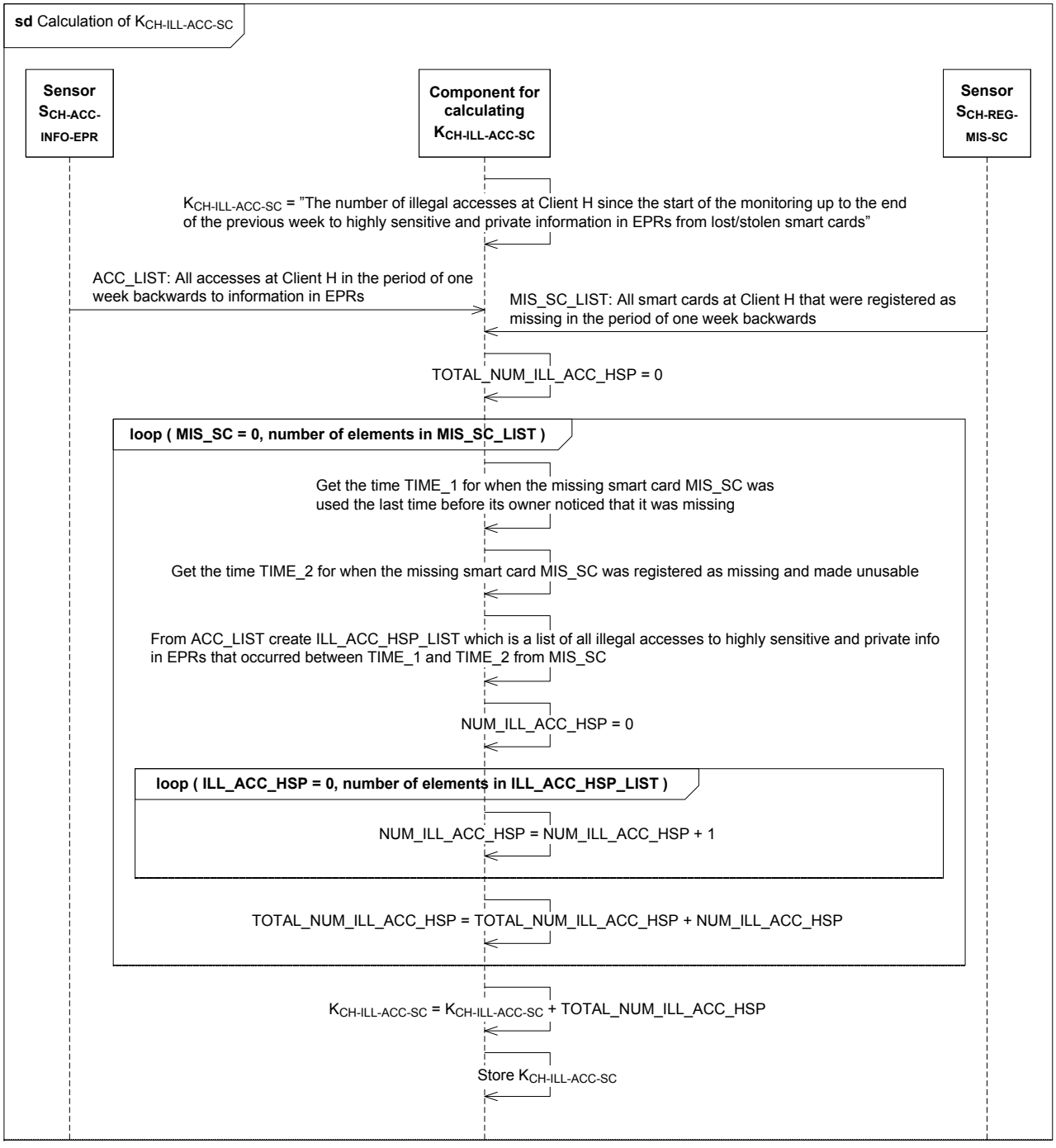

Fig. 24. The sequence diagram "Calculation of $K_{\text{CH-ILL-ACC-SC}}$"

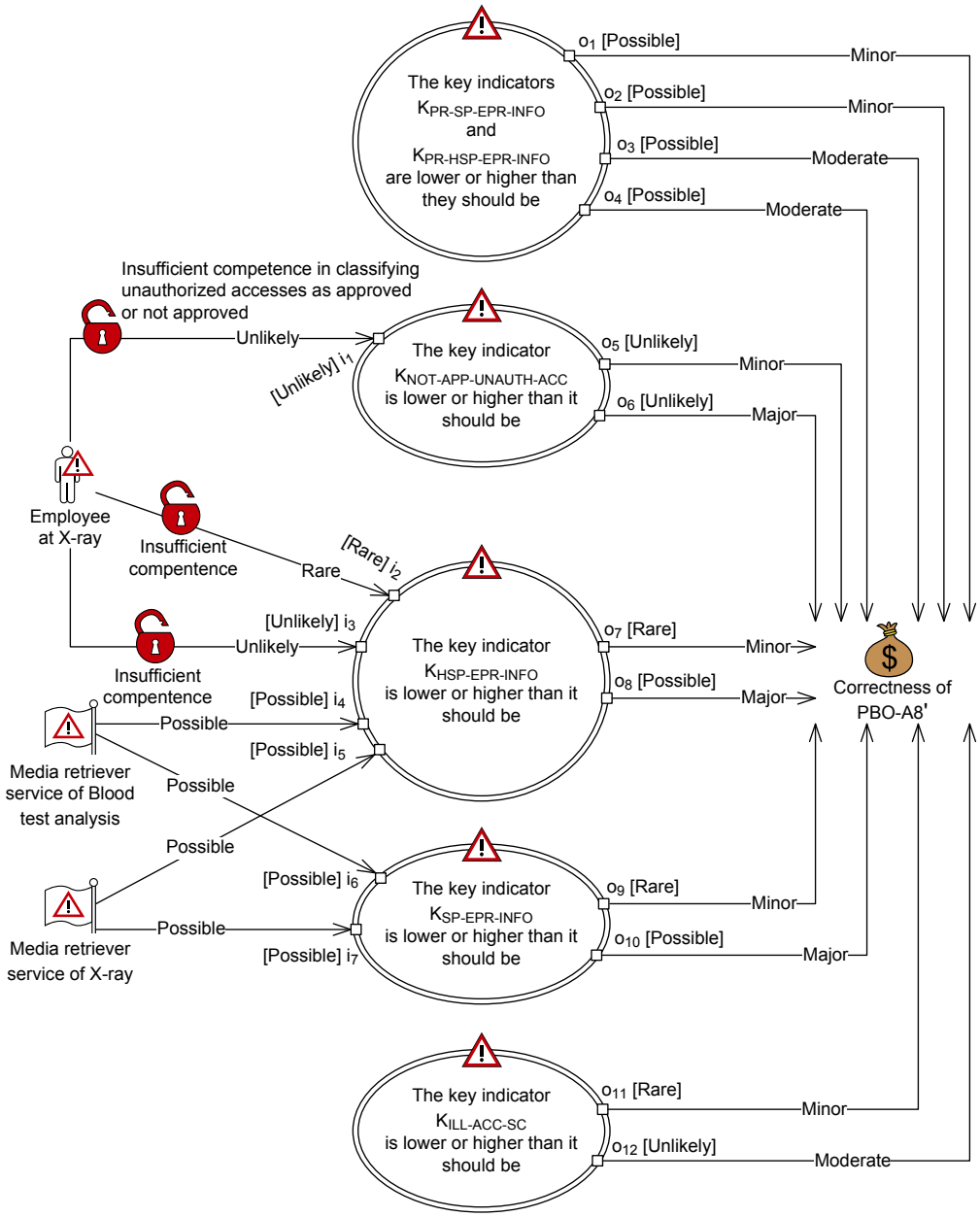

Fig. 25. CORAS threat diagram providing a high-level overview of the impact of the proposed implementation of the monitoring infrastructure for the different composite key indicators on the correctness of PBO-A8'

IX. Evaluate construct validity

To evaluate whether the composite key indicators have construct validity, we re-do the risk analysis from Step 2.2 with the asset "Fulfillment of PBO-A8" replaced by the asset "Correctness of PBO-A8'." We have established that the monitoring infrastructure described in Step 2–4 is suitable for monitoring the relevant part of business. With the designs of the key indicators specified in the previous step, we want to identify in this step whether the proposed implementation of the monitoring infrastructure results in any new unacceptable risks. More precisely, we want to identify unacceptable risks towards the correctness of the reformulated precise business objective that are the result of threats to criteria for construct validity that the different composite key indicators need to fulfill.

We evaluate the construct validity of the composite key indicators based on the criteria given in Section III-F. A high-level overview of the result of the risk analysis is given in the CORAS threat diagram in Fig. 25. In the referenced threat scenarios in Figs. 26 – 30, risk to the correctness of the different composite key indicators have been documented. For the key indicators $K_{\text{PR-SP-EPR-INFO}}$ and $K_{\text{PR-HSP-EPR-INFO}}$, Client H is of the opinion that their

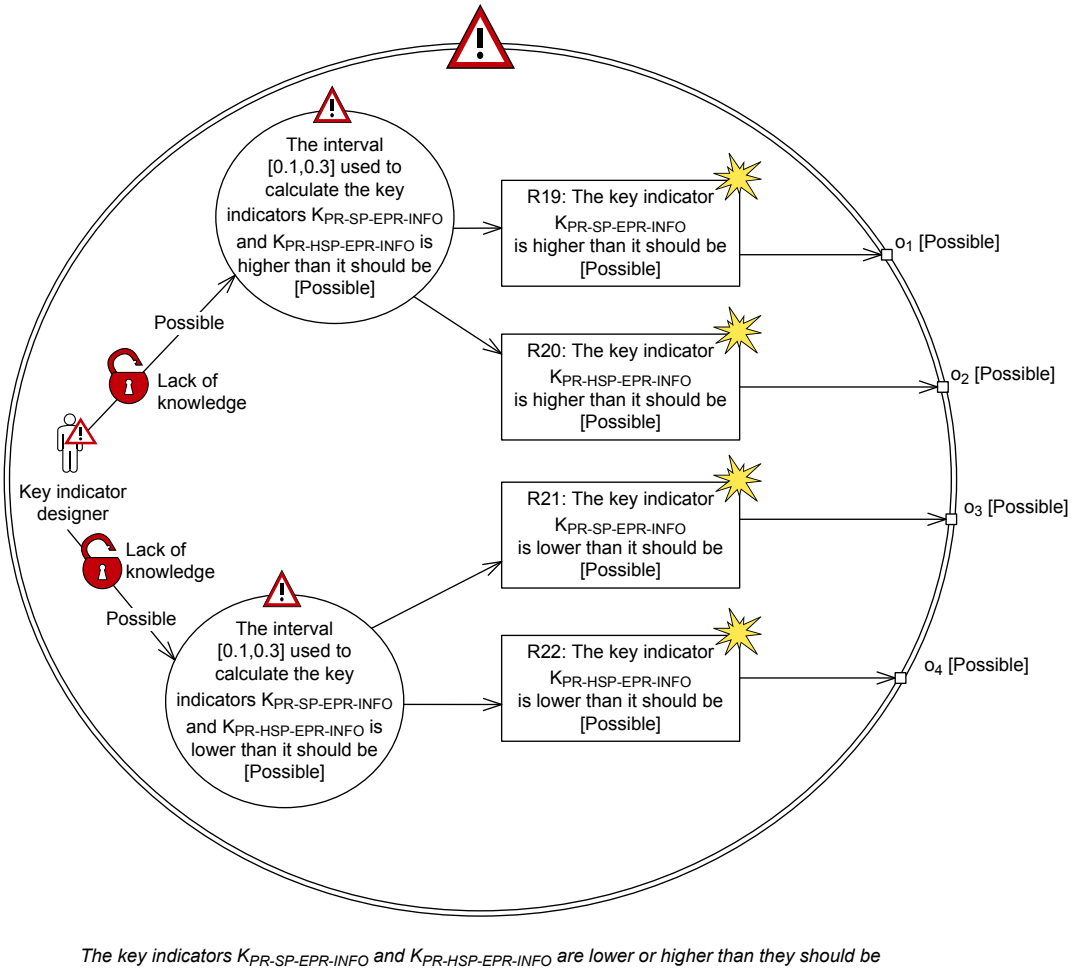

Fig. 26. The referenced threat scenario "The key indicators $K_{\text{PR-SP-EPR-INFO}}$ and $K_{\text{PR-HSP-EPR-INFO}}$ are lower or higher than they should be," referred to in Fig. 25

correctness may be affected if the interval $[0.1, 0.3]$ used to calculate the two key indicators is either too low or too high. This is an example of violation of the stability criterion, since the selection of the interval is the result of human decisions, i.e., expert judgments. For the two composite key indicators, no threats towards the definition and instrument validity of the composite key indicators are identified.

In the case of the key indicator $K_{\text{NOT-APP-UNAUTH-ACC}}$, Client H is of the opinion that its correctness may be affected if the employees who classify unauthorized accesses as approved or not approved at X-ray and Blood test analysis are incompetent and fraudulent, respectively. Both these cases are examples of violation of the stability criterion, since the classification of unauthorized accesses as approved or not approved involves human decisions. Moreover, Client H is worried that the sensor $S_{\text{CH-ACC-INFO-EPR}}$ (represented as a non-human threat in Fig. 27) may be unstable with respect to logging of accesses to information in EPRs. This is an example of violation of the instrument validity criterion. Besides the stability and instrument validity criteria, definition validity should also be evaluated. In our case, we say that a key indicator has definition validity if its design is clear and unambiguous so that the key indicator can be implemented correctly. The only thing that is not clear and unambiguous with respect to the design of $K_{\text{NOT-APP-UNAUTH-ACC}}$ is how unauthorized accesses should be classified as approved or not approved. Since this has already been covered during the evaluation of the stability criterion, we do not pursue this issue further.

In the case of the key indicators $K_{\text{SP-EPR-INFO}}$ and $K_{\text{HSP-EPR-INFO}}$, Client H is worried that the correctness of $K_{\text{SP-EPR-INFO}}$ may be affected if employees at Blood test analysis either fail to identify data leakages of sensitive and private information from EPRs or incorrectly classify sensitive and private information obtained from EPRs as the sources of data leakages, when no such data leakages have occurred. Moreover, Client H is worried that

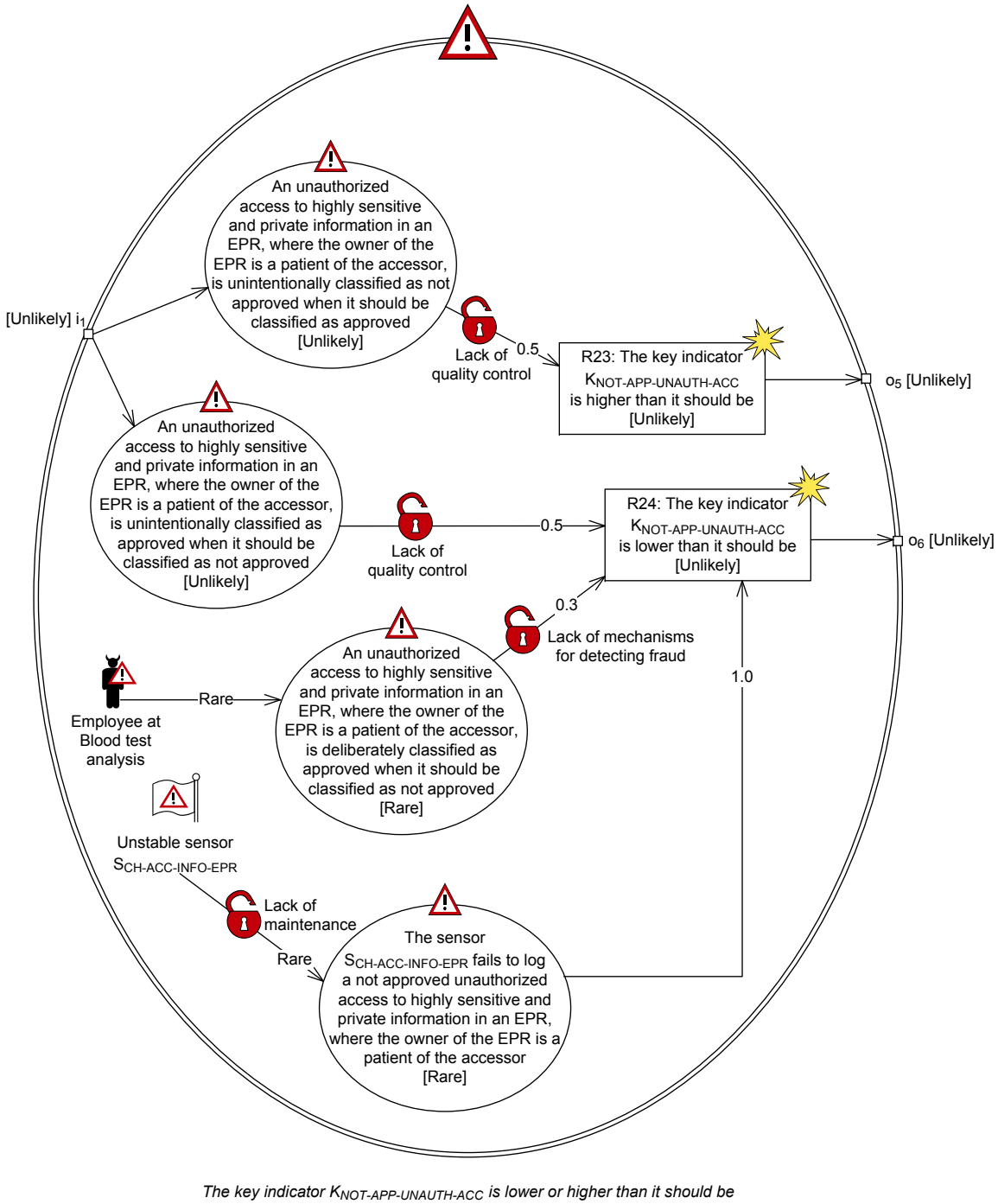

Fig. 27. The referenced threat scenario "The key indicator $K_{\text{NOT-APP-UNAUTH-ACC}}$ is lower or higher than is should be," referred to in Fig. 25

the correctness of $K_{\text{HSP-EPR-INFO}}$ may be affected if employees at X-ray commit the same errors when it comes to highly sensitive and private information in EPRs. Both these cases are examples of violation of the stability criterion. In the case of instrument validity, Client H is worried that the media retriever services employed by Blood test analysis and X-ray are not able to collect the information necessary for detecting data leakages. Client H is also worried that the two composite key indicators may violate the definition validity criterion. The design specifications of the two composite key indicators are not clear and unambiguous with respect to how data leakages should be identified. In both specifications, it is up to the employees investigating potential data leakages to decide. Since this has already been covered during the evaluation of the stability criterion, we do not pursue this issue further.

In the case of the key indicator $K_{\text{ILL-ACC-SC}}$, Client H is worried that its correctness may be affected by health-

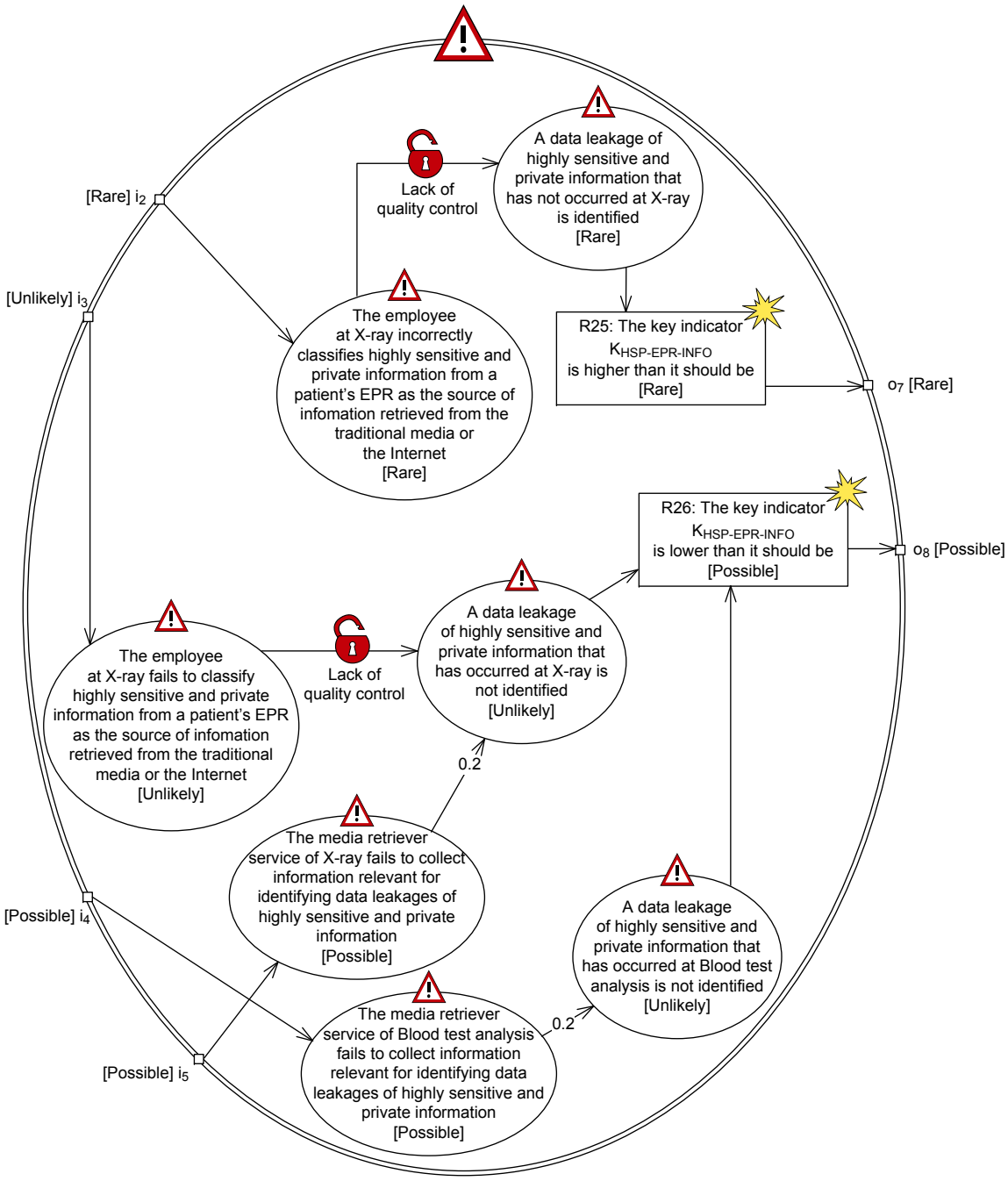

Fig. 28. The referenced threat scenario "The key indicator $K_{\text{HSP-EPR-INFO}}$ is lower or higher than is should be," referred to in Fig. 25

care professionals not having a perfect recollection of when they used their smart cards the last time before losing it. By not having a perfect recollection, accesses to information in EPRs may incorrectly be classified as legal or illegal accesses. This is an example of violation of the stability criterion. For the composite key indicator, no threats towards the definition and instrument validity of the composite key indicator are identified.

In Table XII the risks $R19$ – $R30$ have been plotted according to their likelihoods and consequences. As we can see from the table, the two risks $R26$ and $R28$ are unacceptable. This means that all the composite key indicators with the exceptions of $K_{\text{SP-EPR-INFO}}$ and $K_{\text{HSP-EPR-INFO}}$ have construct validity. As a first step to making these two risks acceptable, Client H finds it necessary to gain more knowledge on the suitability of the two media retriever services. If the two risks do not become acceptable as a result of this, further treatment will be necessary in order

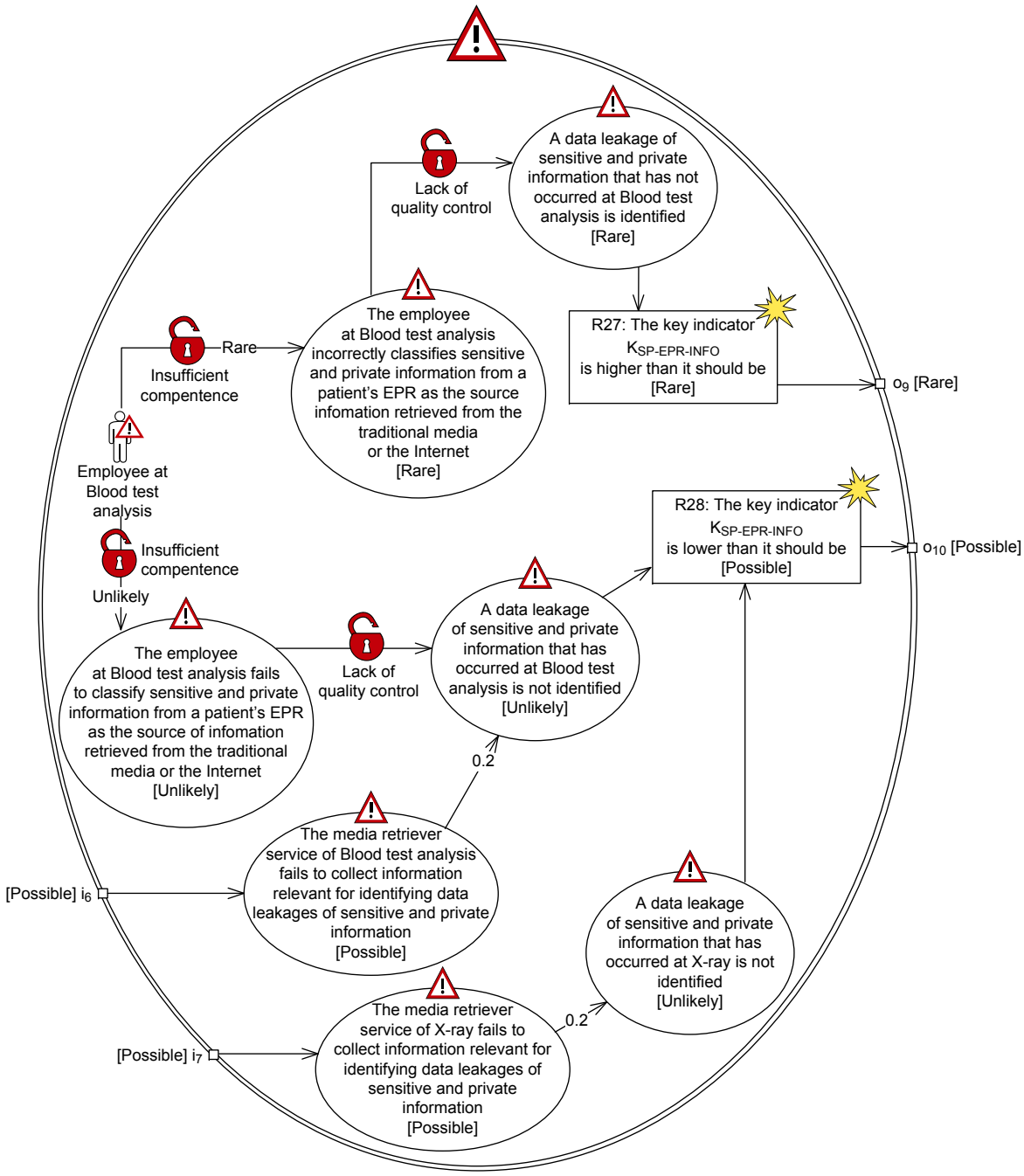

Fig. 29. The referenced threat scenario "The key indicator $K_{\text{SP-EPR-INFO}}$ is lower or higher than is should be," referred to in Fig. 25

for the two key indicators $K_{\text{SP-EPR-INFO}}$ and $K_{\text{HSP-EPR-INFO}}$ to achieve construct validity. Such treatments may involve replacing the media retriever services of Blood test analysis and X-ray, or introducing an additional media retriever service for each of the two hospitals. In the latter case this means that Blood test analysis and X-ray will each identify data leakages based on information which combines results from two media retriever services.

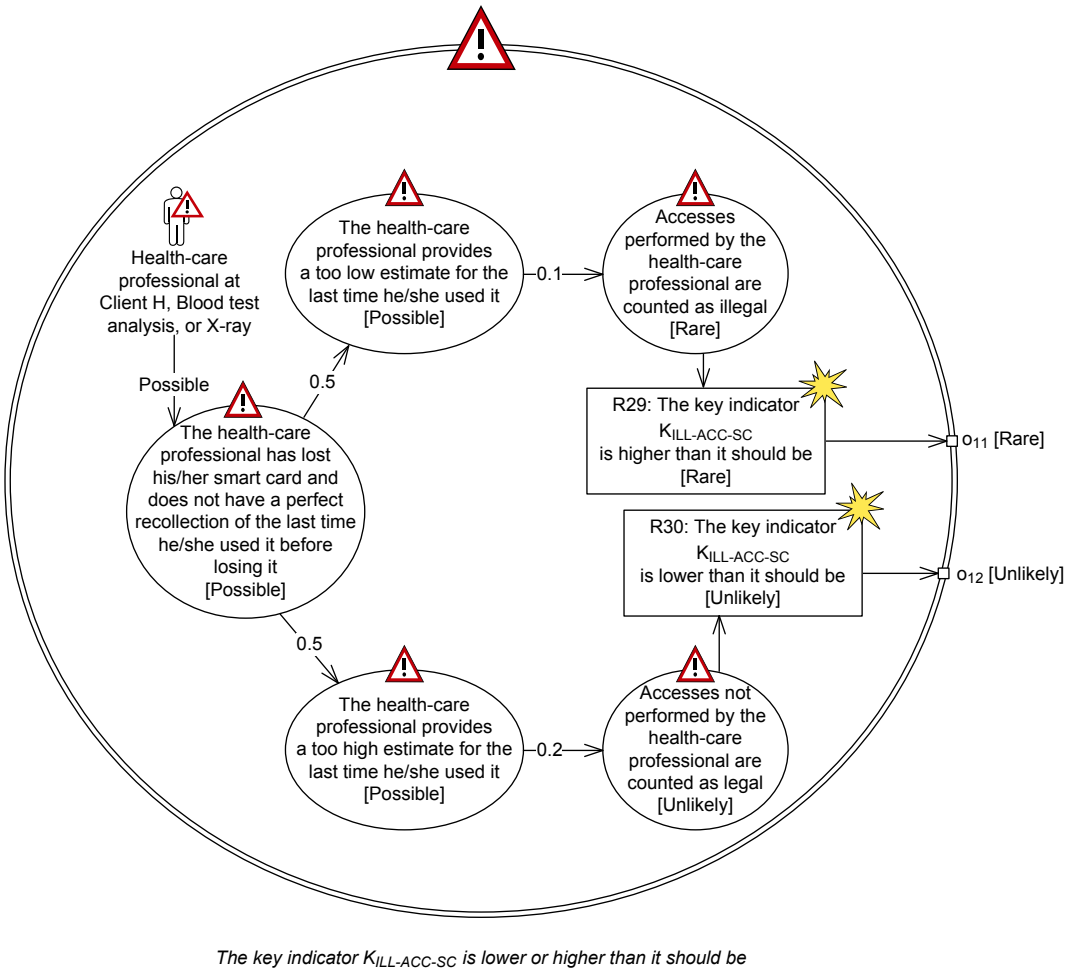

Fig. 30. The referenced threat scenario "The key indicator $K_{\text{ILL-ACC-SC}}$ is lower or higher than is should be," referred to in Fig. 25

TABLE XII
THE RISK EVALUATION MATRIX FROM TABLE XI WITH THE RISKS $R19$ – $R30$ INSERTED

Likelihood \ **Consequence**	Insignificant	Minor	Moderate	Major	Catastrophic
Rare		$R25$, $R27$, $R29$	$R1\&R2'$	$R3\&R4'$, $R8'$, $R10'$, $R15\&R17$	$R12$, $R16\&R18$
Unlikely		$R23$	$R1\&R2''$, $R30$	$R3\&R4''$, $R8''$, $R10''$, $R24$	
Possible		$R6$, $R7$, $R19$, $R20$	$R1\&R2'''$, $R9$, $R11$, $R21$, $R22$	$R26$, $R28$	
Likely	$R13$	$R5$, $R14$			
Certain					

X. Related work

To the best of our knowledge, there exists no other method for the design of valid key indicators to monitor the fulfillment of business objectives with particular focus on quality and ICT-supported monitoring of key indicators. There is a tool-framework called Mozart [23] that uses a model-driven approach to create monitoring applications that employs key performance indicators. We do not focus on the implementation of key indicators, but we specify what is needed for implementing them. The work in [23] also differs from our work by not designing indicators from scratch, but by mining them from a data repository during the design cycle.

An important part of our method is the assessment of the validity of the key indicators we design. Our approach to assessing validity is inspired by research conducted within the software engineering domain. As previously explained, there is however no agreement upon what constitutes a valid software metric [8]. A number of the software metrics validation approaches advocate the use of measurement theory [24][25][26] in the validation (see e.g., [9][27][28]). Measurement theory is a branch of applied mathematics that is useful in measurement and data analysis. The fundamental idea of this theory is that there is a difference between measurements and the attribute being measured. Thus, in order to draw conclusions about the attribute, there is a need to understand the nature of the correspondence between the attribute and the measurements. In [29], an approach that relies on measurement theory for the validation of indicators is presented. This approach uses measurement theory to validate the meaningfulness of IT security risk indicators.

Measurement theory has been criticized of being too rigid and restrictive in a practical measurement setting. Briand et al. [27] advocate a pragmatic approach to measurement theory in software engineering. The authors show that even if their approach may lead to violations of the strict prescriptions and proscriptions of measurement theory, the consequences are small compared to the benefits. Another approach that takes a pragmatic approach to measurement theory is [28]. Here, the authors propose a framework for evaluating software metrics. The applicability of the framework is demonstrated by applying it on a bug count metric.

There exist also approaches that assess the validity of specific sets of key indicators. For instance, in [30] the validity of indicators of firm technological capability is assessed, while the validity of indicators of patent value is assessed in [31].

There are several approaches that focus on measuring the achievement of goals. One example is COBIT [32], which is a framework for IT management and IT governance. The framework provides an IT governance model that helps in delivering value from IT and understanding and managing the risks associated with IT. In the governance model, business goals are aligned with IT goals, while metrics, in the form of leading and lagging indicators [33], and maturity models are used to measure the achievement of the IT goals. In our approach we do not focus on the value that the use of IT has with respect to the business objectives. On the other hand, the risk that the use of IT has with respect to the business objectives is important. In our context, IT is relevant in the sense of providing the infrastructure necessary for monitoring the part of business that needs to fulfill the business objectives. In Step 6 of our method we identify risks that may result from the use of the monitoring infrastructure with respect to the business objectives.

Another way to measure the achievement of goals is by the use of the Goal-Question-Metric [34][35] (GQM) approach. Even though GQM originated as an approach for measuring achievement in software development, it can also be used in other contexts where the purpose is to measure achievement of goals. In GQM, business goals are used to drive the identification of measurement goals. These goals do not necessarily measure the fulfillment of the business goals, but they should always measure something that is of interest to the business. Each measurement goal is refined into questions, while metrics are defined for answering each question. No specific method, beyond reviews, is specified for validating whether the correct questions and metrics have been identified. The data provided by the metrics are interpreted and analyzed with respect to the measurement goal in order to conclude whether it is achieved or not. One of the main differences between our method and GQM is that we characterize precisely what it means to achieve a goal/objective. In GQM, however, this may be a question of interpretation.

In the literature, key indicators are mostly referred to in the context of measuring business performance. There exist numerous approaches to performance measurement. Some of these are presented in [36]. Regardless of the approach being used, the organization must translate their business objectives/goals into a set of key performance indicators in order to measure performance. An approach that is widely used [37] is balanced scorecard [5]. This approach translates the company's vision into four financial and non-financial perspectives. For each perspective a set

of business objectives (strategic goals) and their corresponding key performance indicators are identified. However, the implementation of a balanced scorecard is not necessarily straight forward. In [38], Neely and Bourne identify several reasons for the failure of measurement initiatives such as balanced scorecards. One problem is that the identified measures do not measure fulfillment of the business objectives, while another problem is that measures are identified without putting much thought into how the data must be extracted in order to compute the measures. The first problem can be addressed in Step 4 of our method, while the second problem can be addressed in Step 3 and Step 5 of our method. In Step 3 we identify the sensors to be deployed in the relevant part of business, while in Step 5 we present the kinds of data that needs to be extracted from these sensors in order to compute the measures.

Much research has been done in the field of data quality. The problem of data quality is also recognized within the field of key indicators [39][40]. In [41] a survey on how data quality initiatives are linked with organizational key performance indicators in Australian organizations is presented. This survey shows that a number of organizations do not have data quality initiatives linked to their key indicators. Data quality should be taken into account when designing key indicators, since the use of key indicators based on poor quality data may lead to bad business decisions, which again may greatly harm the organization.

In [42][43] the problem of key indicators computed from uncertain events is investigated. The motivation for this work is to understand the uncertainty of individual key indicators used in business intelligence. The authors use key indicators based on data from multiple domains as examples. In these papers a model for expressing uncertainty is proposed, and a tool for visualizing the uncertain key indicators is presented.

XI. Conclusion

In [1] we presented the method *ValidKI* (Valid Key Indicators) for designing key indicators to monitor the fulfillment of business objectives with particular focus on quality and ICT-supported monitoring of key indicators. ValidKI facilitates the design of a set of key indicators that is valid with respect to a business objective. In this report we have presented the improved and consolidated version of the method.

To the best of our knowledge, there exists no other method for the design of valid key indicators to monitor the fulfillment of business objectives with particular focus on quality and ICT-supported monitoring of key indicators. The applicability of our method has been demonstrated on a large, realistic example case addressing the use of electronic patient records in a hospital environment.

Even though ValidKI has been demonstrated on a large, realistic example case there is still a need to apply ValidKI in a real-world industrial setting in order to evaluate properly to what extent it has the characteristics specified in the introduction. By applying ValidKI in such a setting we will for instance gain more knowledge regarding whether it is time and resource efficient.

Acknowledgments

The research on which this report describes has been carried out within the DIGIT project (180052/S10), funded by the Research Council of Norway, and the MASTER and NESSoS projects, both funded from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreements FP7-216917 and FP7-256980, respectively.

References

[1] O. S. Ligaarden, A. Refsdal, and K. Stølen, "ValidKI: A Method for Designing Key Indicators to Monitor the Fulfillment of Business Objectives," in *Proceedings of First International Conference on Business Intelligence and Technology (BUSTECH'11)*. Wilmington, DE: IARIA, 2011, pp. 57–65.

[2] A. Hammond, A. Adriaanse, E. Rodenburg, D. Bryant, and R. Woodward, *Environmental Indicators: A Systematic Approach to Measuring and Reporting on Environmental Policy Performance in the Context of Sustainable Development*. Washington, DC: World Resources Institute, 1995.

[3] International Organization for Standardization, International Electrotechnical Commission, and Institute of Electrical and Electronics Engineers, "ISO/IEC/IEEE 24765 Systems and Software Engineering – Vocabulary," 2010.

[4] B. Ragland, "Measure, Metrics or Indicator: What's the Difference?" *Crosstalk: The Journal of Defense Software Engineering*, vol. 8, no. 3, 1995.

[5] R. S. Kaplan and D. P. Norton, "The Balanced Scorecard – Measures That Drive Performance," *Harvard Business Review*, vol. 70, no. 1, pp. 71–79, 1992.

[6] Object Management Group, "Unified Modeling Language Specification, Version 2.0," 2004.

[7] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 9126 Information Technology – Software Product Evaluation – Quality Characteristics and Guidelines for their Use," 1991.

[8] A. Meneely, B. Smith, and L. Williams, "Software Metrics Validation Criteria: A Systematic Literature Review," Department of Computer Science, North Carolina State University, Raleigh, NC, Tech. Rep. TR-2010-2, 2010.

[9] A. L. Baker, J. M. Bieman, N. E. Fenton, D. A. Gustafson, A. Melton, and R. W. Whitty, "A Philosophy for Software Measurement," *Journal of Systems and Software*, vol. 12, no. 3, pp. 277–281, 1990.

[10] B. Kitchenham, S. L. Pfleeger, and N. Fenton, "Towards a Framework for Software Measurement Validation," *IEEE Transactions on Software Engineering*, vol. 21, no. 12, pp. 929–944, 1995.

[11] J. M. Roche, "Software Metrics and Measurement Principles," *ACM SIGSOFT Software Engineering Notes*, vol. 19, no. 1, pp. 77–85, 1994.

[12] B. Curtis, "Measurement and Experimentation in Software Engineering," *Proceedings of the IEEE*, vol. 68, no. 9, pp. 1144–1157, 1980.

[13] B. Henderson-Sellers, "The Mathematical Validity of Software Metrics," *ACM SIGSOFT Software Engineering Notes*, vol. 21, no. 5, pp. 89–94, 1996.

[14] N. E. Fenton, "Software Measurement: A Necessary Scientific Basis," *IEEE Transactions on Software Engineering*, vol. 20, no. 3, pp. 199–206, 1994.

[15] K. El-Emam, "A Methodology for Validating Software Product Metrics," National Research Council of Canada, Ottawa, ON, Tech. Rep. NCR/ERC-1076, 2000.

[16] J. P. Cavano and J. A. McCall, "A Framework for the Measurement of Software Quality," in *Proceedings of the Software Quality Assurance Workshop on Functional and Performance Issues*. New York, NY: ACM Press, 1978, pp. 133–139.

[17] R. Lincke and W. Lowe, "Foundations for Defining Software Metrics," in *Proceedings of 3rd International Workshop on Metamodels, Schemas, Grammars, and Ontologies (ateM'06) for Reverse Engineering*. Mainz: Johannes Gutenberg-Universität Mainz, 2006.

[18] M. E. Bush and N. E. Fenton, "Software Measurement: A Conceptual Framework," *Journal of Systems and Software*, vol. 12, no. 3, pp. 223–231, 1990.

[19] Council of Europe, "Convention for the Protection of Human Rights and Fundamental Freedoms," 1954.

[20] European Court of Human Rights, "Press Release – Chamber Judgments 17.07.08," 17. July 2008.

[21] Helsedirektoratet, "Code of Conduct for Information Security – The Healthcare, Care, and Social Services Sector," http://www.helsedirektoratet.no/publikasjoner/norm-for-informasjonssikkerhet/Publikasjoner/code-of-conduct-for-information-security.pdf, Accessed: 2012-06-21, 2. June 2010.

[22] M. S. Lund, B. Solhaug, and K. Stølen, *Model-Driven Risk Analysis: The CORAS Approach*, 1st ed. Berlin/Heidelberg: Springer-Verlag, 2010.

[23] M. Abe, J. Jeng, and Y. Li, "A Tool Framework for KPI Application Development," in *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'07)*. Los Alamitos, CA: IEEE Computer Society, 2007, pp. 22–29.

[24] D. H. Krantz, R. D. Luce, P. Suppes, and A. Tversky, *Foundations of Measurement, Vol. I: Additive and Polynomial Representations*. New York, NY: Academic Press, 1971.

[25] P. Suppes, D. H. Krantz, R. D. Luce, and A. Tversky, *Foundations of Measurement, Vol. II: Geometrical, Threshold, and Probabilistic Representations*. New York, NY: Academic Press, 1989.

[26] R. D. Luce, D. H. Krantz, P. Suppes, and A. Tversky, *Foundations of Measurement, Vol. III: Representation, Axiomatization, and Invariance*. New York, NY: Academic Press, 1990.

[27] L. Briand, K. El-Emam, and S. Morasca, "On the Application of Measurement Theory in Software Engineering," *Empirical Software Engineering*, vol. 1, no. 1, pp. 61–88, 1996.

[28] C. Kaner and W. P. Bond, "Software Engineering Metrics: What Do They Measure and How Do We Know?" in *Proceedings of 10th International Software Metrics Symposium (METRICS'04)*. Los Alamitos, CA: IEEE Computer Society, 2004.

[29] A. Morali and R. Wieringa, "Towards Validating Risk Indicators Based on Measurement Theory," in *Proceedings of First International Workshop on Risk and Trust in Extended Enterprises*. Los Alamitos, CA: IEEE Computer Society, 2010, pp. 443–447.

[30] T. Schoenecker and L. Swanson, "Indicators of Firm Technological Capability: Validity and Performance Implications," *IEEE Transactions on Engineering Management*, vol. 49, no. 1, pp. 36–44, 2002.

[31] M. Reitzig, "Improving Patent Valuations for Management Purposes – Validating New Indicators by Analyzing Application Rationales," *Research Policy*, vol. 33, no. 6-7, pp. 939–957, 2004.

[32] IT Governance Institute, "COBIT 4.1," 2007.

[33] W. Jansen, *Directions in Security Metrics Research*. Darby, PA: DIANE Publishing, 2010.

[34] V. R. Basili and D. M. Weiss, "A Methodology for Collecting Valid Software Engineering Data," *IEEE Transactions on Software Engineering*, vol. SE-10, no. 6, pp. 728–738, 1984.

[35] R. V. Solingen and E. Berghout, *The Goal/Question/Metric method: A Practical Guide for Quality Improvement of Software Development*. New York, NY: McGraw-Hill International, 1999.

[36] A. Neely, J. Mills, K. Platts, H. Richards, M. Gregory, M. Bourne, and M. Kennerley, "Performance Measurement System Design: Developing and Testing a Process-based Approach," *International Journal of Operation & Production Management*, vol. 20, no. 10, pp. 1119–1145, 2000.

[37] T. Lester, "Measure for Measure," http://www.ft.com/cms/s/2/31e6b750-16e9-11d9-a89a-00000e2511c8.html#axzz1ImHJOLmg, Accessed: 2012-06-21, 5. October 2004.

[38] A. Neely and M. Bourne, "Why Measurement Initiatives Fail," *Measuring Business Excellence*, vol. 4, no. 4, pp. 3–6, 2000.

[39] S. M. Bird, D. Cox, V. T. Farewell, H. Goldstein, T. Holt, and P. C. Smith, "Performance Indicators: Good, Bad, and Ugly," *Journal Of The Royal Statistical Society. Series A (Statistics in Society)*, vol. 168, no. 1, pp. 1–27, 2005.

[40] D. M. Eddy, "Performance Measurement: Problems and Solutions," *Health Affairs*, vol. 17, no. 4, pp. 7–25, 1998.

[41] V. Masayna, A. Koronios, and J. Gao, "A Framework for the Development of the Business Case for the Introduction of Data Quality Program Linked to Corporate KPIs & Governance," in *Proceedings of the 2009 Fourth International Conference on Cooperation and Promotion of Information Resources in Science and Technology (COINFO'09)*. Los Alamitos, CA: IEEE Computer Society, 2009, pp. 230–235.

[42] C. Rodríguez, F. Daniel, F. Casati, and C. Cappiello, "Computing Uncertain Key Indicators from Uncertain Data," in *Proceedings of 14th International Conference on Information Quality (ICIQ'09)*. Potsdam/Cambridge, MA: HPI/MIT, 2009, pp. 106–120.

[43] C. Rodríguez, F. Daniel, F. Casati, and C. Cappiello, "Toward Uncertain Business Intelligence: The Case of Key Indicators," *Internet Computing*, vol. 14, no. 4, pp. 32–40, 2010.

Technology for a better society

www.sintef.no